Enterasys Matrix®
DFE-Gold

Configuration Guide
Firmware Version 6.11.xx

P/N 9033933-15

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

Notice

Enterasys Networks reserves the right to make changes in specifications and other information contained in this document and its web site without prior notice. The reader should in all cases consult Enterasys Networks to determine whether any such changes have been made.

The hardware, firmware, or software described in this document is subject to change without notice.

IN NO EVENT SHALL ENTERASYS NETWORKS BE LIABLE FOR ANY INCIDENTAL, INDIRECT, SPECIAL, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING BUT NOT LIMITED TO LOST PROFITS) ARISING OUT OF OR RELATED TO THIS DOCUMENT, WEB SITE, OR THE INFORMATION CONTAINED IN THEM, EVEN IF ENTERASYS NETWORKS HAS BEEN ADVISED OF, KNEW OF, OR SHOULD HAVE KNOWN OF, THE POSSIBILITY OF SUCH DAMAGES.

Enterasys Networks, Inc.
50 Minuteman Road
Andover, MA 01810

© 2008 Enterasys Networks, Inc. All rights reserved.

Part Number: 9033933-15 September 2008

ENTERASYS, ENTERASYS NETWORKS, ENTERASYS MATRIX, ENTERASYS NETSIGHT, LANVIEW, WEBVIEW, and any logos associated therewith, are trademarks or registered trademarks of Enterasys Networks, Inc., in the United States and other countries. For a complete list of Enterasys trademarks, see http://www.enterasys.com/company/trademarks.aspx.

All other product names mentioned in this manual may be trademarks or registered trademarks of their respective companies.

Documentation URL: http://www.enterasys.com/support/manuals

Documentacion URL: http://www.enterasys.com/support/manuals

Dokumentation im Internet: http://www.enterasys.com/support/manuals

Downloaded from www.Manualslib.com manuals search engine

Enterasys Networks, Inc. Software License Agreement

This document is an agreement ("Agreement") between You, the end user, and Enterasys Networks, Inc. on behalf of itself and its Affiliates ("Enterasys") that sets forth your rights and obligations with respect to the software contained in CD-ROM or other media. "Affiliates" means any person, partnership, corporation, limited liability company, or other form of enterprise that directly or indirectly through one or more intermediaries, controls, or is controlled by, or is under common control with the party specified. BY INSTALLING THE ENCLOSED PRODUCT, YOU ARE AGREEING TO BECOME BOUND BY THE TERMS OF THIS AGREEMENT, WHICH INCLUDES THE LICENSE AND THE LIMITATION OF WARRANTY AND DISCLAIMER OF LIABILITY. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, RETURN THE UNOPENED PRODUCT TO ENTERASYS OR YOUR DEALER, IF ANY, WITHIN TEN (10) DAYS FOLLOWING THE DATE OF RECEIPT FOR A FULL REFUND.

IF YOU HAVE ANY QUESTIONS ABOUT THIS AGREEMENT, CONTACT ENTERASYS NETWORKS, INC. (978) 684-1000. Attn: Legal Department.

Enterasys will grant You a non-transferable, non-exclusive license to use the machine-readable form of software (the "Licensed Software") and the accompanying documentation (the Licensed Software, the media embodying the Licensed Software, and the documentation are collectively referred to in this Agreement as the "Licensed Materials") on one single computer if You agree to the following terms and conditions:

1. **TERM.** This Agreement is effective from the date on which You open the package containing the Licensed Materials. You may terminate the Agreement at any time by destroying the Licensed Materials, together with all copies, modifications and merged portions in any form. The Agreement and your license to use the Licensed Materials will also terminate if You fail to comply with any term or condition herein.

2. **GRANT OF SOFTWARE LICENSE.** The license granted to You by Enterasys when You open this sealed package authorizes You to use the Licensed Software on any one, single computer only, or any replacement for that computer, for internal use only. A separate license, under a separate Software License Agreement, is required for any other computer on which You or another individual or employee intend to use the Licensed Software. YOU MAY NOT USE, COPY, OR MODIFY THE LICENSED MATERIALS, IN WHOLE OR IN PART, EXCEPT AS EXPRESSLY PROVIDED IN THIS AGREEMENT.

3. **RESTRICTION AGAINST COPYING OR MODIFYING LICENSED MATERIALS**. Except as expressly permitted in this Agreement, You may not copy or otherwise reproduce the Licensed Materials. In no event does the limited copying or reproduction permitted under this Agreement include the right to decompile, disassemble, electronically transfer, or reverse engineer the Licensed Software, or to translate the Licensed Software into another computer language.

The media embodying the Licensed Software may be copied by You, in whole or in part, into printed or machine readable form, in sufficient numbers only for backup or archival purposes, or to replace a worn or defective copy. However, You agree not to have more than two (2) copies of the Licensed Software in whole or in part, including the original media, in your possession for said purposes without Enterasys' prior written consent, and in no event shall You operate more than one copy of the Licensed Software. You may not copy or reproduce the documentation. You agree to maintain appropriate records of the location of the original media and all copies of the Licensed Software, in whole or in part, made by You. You may modify the machine-readable form of the Licensed Software for (1) your own internal use or (2) to merge the Licensed Software into other program material to form a modular work for your own use, provided that such work remains modular, but on termination of this Agreement, You are required to completely remove the Licensed Software from any such modular work. Any portion of the Licensed Software included in any such modular work shall be used only on a single computer for internal purposes and shall remain subject to all the terms and conditions of this Agreement.

You agree to include any copyright or other proprietary notice set forth on the label of the media embodying the Licensed Software on any copy of the Licensed Software in any form, in whole or in part, or on any modification of the Licensed Software or any such modular work containing the Licensed Software or any part thereof.

4. **TITLE AND PROPRIETARY RIGHTS**.

   (a) The Licensed Materials are copyrighted works and are the sole and exclusive property of Enterasys, any company or a division thereof which Enterasys controls or is controlled by, or which may result from the merger or consolidation with Enterasys (its "Affiliates"), and/or their suppliers. This Agreement conveys a limited right to operate the Licensed Materials and shall not be construed to convey title to the Licensed Materials to You. There are no implied rights. You shall not sell, lease, transfer, sublicense, dispose of, or otherwise make available the Licensed Materials or any portion thereof, to any other party.

   (b) You further acknowledge that in the event of a breach of this Agreement, Enterasys shall suffer severe and irreparable damages for which monetary compensation alone will be inadequate. You therefore agree that in the event of a breach of this Agreement, Enterasys shall be entitled to monetary damages and its reasonable attorney's fees and costs in enforcing this Agreement, as well as injunctive relief to restrain such breach, in addition to any other remedies available to Enterasys.

Downloaded from www.Manualslib.com manuals search engine

5. **PROTECTION AND SECURITY**. In the performance of this Agreement or in contemplation thereof, You and your employees and agents may have access to private or confidential information owned or controlled by Enterasys relating to the Licensed Materials supplied hereunder including, but not limited to, product specifications and schematics, and such information may contain proprietary details and disclosures. All information and data so acquired by You or your employees or agents under this Agreement or in contemplation hereof shall be and shall remain Enterasys' exclusive property, and You shall use your best efforts (which in any event shall not be less than the efforts You take to ensure the confidentiality of your own proprietary and other confidential information) to keep, and have your employees and agents keep, any and all such information and data confidential, and shall not copy, publish, or disclose it to others, without Enterasys' prior written approval, and shall return such information and data to Enterasys at its request. Nothing herein shall limit your use or dissemination of information not actually derived from Enterasys or of information which has been or subsequently is made public by Enterasys, or a third party having authority to do so.

You agree not to deliver or otherwise make available the Licensed Materials or any part thereof, including without limitation the object or source code (if provided) of the Licensed Software, to any party other than Enterasys or its employees, except for purposes specifically related to your use of the Licensed Software on a single computer as expressly provided in this Agreement, without the prior written consent of Enterasys. You agree to use your best efforts and take all reasonable steps to safeguard the Licensed Materials to ensure that no unauthorized personnel shall have access thereto and that no unauthorized copy, publication, disclosure, or distribution, in whole or in part, in any form shall be made, and You agree to notify Enterasys of any unauthorized use thereof. You acknowledge that the Licensed Materials contain valuable confidential information and trade secrets, and that unauthorized use, copying and/or disclosure thereof are harmful to Enterasys or its Affiliates and/or its/their software suppliers.

6. **MAINTENANCE AND UPDATES**. Updates and certain maintenance and support services, if any, shall be provided to You pursuant to the terms of an Enterasys Service and Maintenance Agreement, if Enterasys and You enter into such an agreement. Except as specifically set forth in such agreement, Enterasys shall not be under any obligation to provide Software Updates, modifications, or enhancements, or Software maintenance and support services to You.

7. **DEFAULT AND TERMINATION**. In the event that You shall fail to keep, observe, or perform any obligation under this Agreement, including a failure to pay any sums due to Enterasys, or in the event that You become insolvent or seek protection, voluntarily or involuntarily, under any bankruptcy law, Enterasys may, in addition to any other remedies it may have under law, terminate the License and any other agreements between Enterasys and You.

(a) Immediately after any termination of the Agreement or if You have for any reason discontinued use of Software, You shall return to Enterasys the original and any copies of the Licensed Materials and remove the Licensed Software from any modular works made pursuant to Section 3, and certify in writing that through your best efforts and to the best of your knowledge the original and all copies of the terminated or discontinued Licensed Materials have been returned to Enterasys.

(b) Sections 4, 5, 7, 8, 9, 10, 11, and 12 shall survive termination of this Agreement for any reason.

8. **EXPORT REQUIREMENTS**. You understand that Enterasys and its Affiliates are subject to regulation by agencies of the U.S. Government, including the U.S. Department of Commerce, which prohibit export or diversion of certain technical products to certain countries, unless a license to export the product is obtained from the U.S. Government or an exception from obtaining such license may be relied upon by the exporting party.

If the Licensed Materials are exported from the United States pursuant to the License Exception CIV under the U.S. Export Administration Regulations, You agree that You are a civil end user of the Licensed Materials and agree that You will use the Licensed Materials for civil end uses only and not for military purposes.

If the Licensed Materials are exported from the United States pursuant to the License Exception TSR under the U.S. Export Administration Regulations, in addition to the restriction on transfer set forth in Section 4 of this Agreement, You agree not to (i) reexport or release the Licensed Software, the source code for the Licensed Software or technology to a national of a country in Country Groups D:1 or E:2 (Albania, Armenia, Azerbaijan, Belarus, Cambodia, Cuba, Georgia, Iraq, Kazakhstan, Kyrgyzstan, Laos, Libya, Macau, Moldova, Mongolia, North Korea, the People's Republic of China, Russia, Tajikistan, Turkmenistan, Ukraine, Uzbekistan, Vietnam, or such other countries as may be designated by the United States Government), (ii) export to Country Groups D:1 or E:2 (as defined herein) the direct product of the Licensed Software or the technology, if such foreign produced direct product is subject to national security controls as identified on the U.S. Commerce Control List, or (iii) if the direct product of the technology is a complete plant o r any major component of a plant, export to Country Groups D:1 or E:2 the direct product of the plant or a major component thereof, if such foreign produced direct product is subject to national security controls as identified on the U.S. Commerce Control List or is subject to State Department controls under the U.S. Munitions List.

Downloaded from www.Manualslib.com manuals search engine

9. **UNITED STATES GOVERNMENT RESTRICTED RIGHTS**. The Licensed Materials (i) were developed solely at private expense; (ii) contains "restricted computer software" submitted with restricted rights in accordance with section 52.227-19 (a) through (d) of the Commercial Computer Software-Restricted Rights Clause and its successors, and (iii) in all respects is proprietary data belonging to Enterasys and/or its suppliers. For Department of Defense units, the Licensed Materials are considered commercial computer software in accordance with DFARS section 227.7202-3 and its successors, and use, duplication, or disclosure by the U.S. Government is subject to restrictions set forth herein.

10. **LIMITED WARRANTY AND LIMITATION OF LIABILITY**. The only warranty Enterasys makes to You in connection with this license of the Licensed Materials is that if the media on which the Licensed Software is recorded is defective, it will be replaced without charge, if Enterasys in good faith determines that the media and proof of payment of the license fee are returned to Enterasys or the dealer from whom it was obtained within ninety (90) days of the date of payment of the license fee.

NEITHER ENTERASYS NOR ITS AFFILIATES MAKE ANY OTHER WARRANTY OR REPRESENTATION, EXPRESS OR IMPLIED, WITH RESPECT TO THE LICENSED MATERIALS, WHICH ARE LICENSED "AS IS". THE LIMITED WARRANTY AND REMEDY PROVIDED ABOVE ARE EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, INCLUDING IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE EXPRESSLY DISCLAIMED, AND STATEMENTS OR REPRESENTATIONS MADE BY ANY OTHER PERSON OR FIRM ARE VOID. ONLY TO THE EXTENT SUCH EXCLUSION OF ANY IMPLIED WARRANTY IS NOT PERMITTED BY LAW, THE DURATION OF SUCH IMPLIED WARRANTY IS LIMITED TO THE DURATION OF THE LIMITED WARRANTY SET FORTH ABOVE. YOU ASSUME ALL RISK AS TO THE QUALITY, FUNCTION AND PERFORMANCE OF THE LICENSED MATERIALS. IN NO EVENT WILL ENTERASYS OR ANY OTHER PARTY WHO HAS BEEN INVOLVED IN THE CREATION, PRODUCTION OR DELIVERY OF THE LICENSED MATERIALS BE LIABLE FOR SPECIAL, DIRECT, INDIRECT, RELIANCE, INCIDENTAL OR CONSEQUENTIAL DAMAGES, INCLUDING LOSS OF DATA OR PROFITS OR FOR INABILITY TO USE THE LICENSED MATERIALS, TO ANY PARTY EVEN IF ENTERASYS OR SUCH OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT SHALL ENTERASYS OR SUCH OTHER PARTY'S LIABILITY FOR ANY DAMAGES OR LOSS TO YOU OR ANY OTHER PARTY EXCEED THE LICENSE FEE YOU PAID FOR THE LICENSED MATERIALS.

Some states do not allow limitations on how long an implied warranty lasts and some states do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation and exclusion may not apply to You. This limited warranty gives You specific legal rights, and You may also have other rights which vary from state to state.

11. **JURISDICTION**. The rights and obligations of the parties to this Agreement shall be governed and construed in accordance with the laws and in the State and Federal courts of the Commonwealth of Massachusetts, without regard to its rules with respect to choice of law. You waive any objections to the personal jurisdiction and venue of such courts. None of the 1980 United Nations Convention on the Limitation Period in the International Sale of Goods, and the Uniform Computer Information Transactions Act shall apply to this Agreement.

12. **GENERAL**.

(a) This Agreement is the entire agreement between Enterasys and You regarding the Licensed Materials, and all prior agreements, representations, statements, and undertakings, oral or written, are hereby expressly superseded and canceled.

(b) This Agreement may not be changed or amended except in writing signed by both parties hereto.

(c) You represent that You have full right and/or authorization to enter into this Agreement.

(d) This Agreement shall not be assignable by You without the express written consent of Enterasys, The rights of Enterasys and Your obligations under this Agreement shall inure to the benefit of Enterasys' assignees, licensors, and licensees.

(e) Section headings are for convenience only and shall not be considered in the interpretation of this Agreement.

(f) The provisions of the Agreement are severable and if any one or more of the provisions hereof are judicially determined to be illegal or otherwise unenforceable, in whole or in part, the remaining provisions of this Agreement shall nevertheless be binding on and enforceable by and between the parties hereto.

(g) Enterasys' waiver of any right shall not constitute waiver of that right in future. This Agreement constitutes the entire understanding between the parties with respect to the subject matter hereof, and all prior agreements, representations, statements and undertakings, oral or written, are hereby expressly superseded and canceled. No purchase order shall supersede this Agreement.

(h) Should You have any questions regarding this Agreement, You may contact Enterasys at the address set forth below. Any notice or other communication to be sent to Enterasys must be mailed by certified mail to the following address: ENTERASYS NETWORKS, INC., 50 Minuteman Road, Andover, MA 01810 Attn: Manager - Legal Department.

Downloaded from www.Manualslib.com manuals search engine

Contents

About This Guide

Using This Guide xxxiii
Structure of This Guide xxxiii
Related Documents xxxv
Conventions Used in This Guide xxxv
Getting Help xxxvi

Chapter 1: Introduction

Matrix DFE Series Features 1-1
Matrix Series CLI Overview 1-1
Device Management Methods 1-2

Chapter 2: Startup and General Configuration

Startup and General Configuration Summary 2-1
Factory Default Settings 2-1
CLI “Defaults” Descriptions 2-6
CLI Command Modes 2-6
Using WebView 2-7
Starting and Navigating the Command Line Interface 2-7
Configuring the Line Editor 2-11
Commands 2-13
show line-editor 2-13
set line-editor 2-14
Setting User Accounts and Passwords 2-15
Purpose 2-15
Commands 2-15
show system login 2-15
set system login 2-16
clear system login 2-17
set password 2-18
show system password 2-19
set system password 2-20
clear system password 2-22
show system lockout 2-23
set system lockout 2-24
Managing the Management Authentication Notification MIB 2-26
Purpose 2-26
Commands 2-26
show mgmt-auth-notify 2-26
set mgmt-auth-notify 2-27
clear mgmt-auth-notify 2-28
Setting Basic Device Properties 2-30
Purpose 2-30
Commands 2-30
show ip address 2-31
set ip address 2-31
clear ip address 2-32
show ip gratuitous-arp 2-32
set ip gratuitous-arp 2-33

Downloaded from www.Manualslib.com manuals search engine

clear ip gratuitous-arp 2-33
show system 2-34
show system hardware 2-35
show system utilization 2-37
set system utilization threshold 2-39
clear system utilization 2-40
show time 2-40
set time 2-41
show summertime 2-41
set summertime 2-42
set summertime date 2-42
set summertime recurring 2-43
clear summertime 2-44
set prompt 2-44
set cli completion 2-45
loop 2-45
show banner 2-46
set banner 2-47
clear banner 2-48
show version 2-48
set system name 2-50
set system location 2-50
set system contact 2-51
set width 2-51
set length 2-52
show logout 2-52
set logout 2-53
show physical alias 2-53
set physical alias 2-54
clear physical alias 2-55
show physical assetid 2-55
set physical assetid 2-56
clear physical assetid 2-56
Activating Licensed Features 2-58
About Redundant Management on Matrix DFE-Gold Series Modules 2-58
Purpose 2-58
Commands 2-58
set license 2-58
show license 2-59
clear license 2-60
Configuring Power over Ethernet (PoE) 2-61
Purpose 2-61
Commands 2-61
show inlinepower 2-61
set inlinepower mode 2-62
clear inlinepower mode 2-63
set inlinepower available 2-63
clear inlinepower available 2-64
set inlinepower powertrap 2-65
clear inlinepower powertrap 2-65
set inlinepower assigned 2-66
clear inlinepower assigned 2-66
set inlinepower threshold 2-67
clear inlinepower threshold 2-67
set inlinepower management 2-68
clear inlinepower management 2-68

Downloaded from www.Manualslib.com manuals search engine

set inlinepower psetrap 2-69
clear inlinepower psetrap 2-69
show port inlinepower 2-70
set port inlinepower 2-70
clear port inlinepower 2-71
Reviewing and Selecting a Boot Firmware Image 2-72
Downloading a New Firmware Image 2-72
Purpose 2-74
Commands 2-74
show boot system 2-74
set boot system 2-75
Starting and Configuring Telnet 2-76
Purpose 2-76
Commands 2-76
show telnet 2-76
set telnet 2-77
telnet 2-77
show router telnet 2-78
set router telnet 2-78
clear router telnet 2-79
Managing Configuration and Image Files 2-80
Purpose 2-80
Commands 2-80
dir 2-81
show file 2-83
show config 2-85
configure 2-86
copy 2-86
delete 2-87
script 2-88
Enabling or Disabling the Path MTU Discovery Protocol 2-90
Purpose 2-90
Commands 2-90
show mtu 2-90
set mtu 2-91
clear mtu 2-91
Pausing, Clearing and Closing the CLI 2-92
Purpose 2-92
Commands 2-92
cls (clear screen) 2-92
exit | quit 2-92
Resetting the Device 2-94
Purpose 2-94
Commands 2-94
show reset 2-94
reset 2-95
reset at 2-96
reset in 2-96
clear config 2-97
Gathering Technical Support Information 2-98
Purpose 2-98
Command 2-98
show support 2-98
Preparing the Device for Router Mode 2-100
Pre-Routing Configuration Tasks 2-100
Reviewing and Configuring Routing 2-101

Downloaded from www.Manualslib.com manuals search engine

Purpose 2-101
Commands 2-101
show router 2-102
clear router 2-102
router 2-103
Enabling Router Configuration Modes 2-103

Chapter 3: Discovery Protocols Configuration

Displaying Neighbors 3-1
Purpose 3-1
Command 3-1
show neighbors 3-1
Enterasys Discovery Protocol 3-3
Purpose 3-3
Commands 3-3
show cdp 3-3
set cdp state 3-4
set cdp auth 3-5
set cdp interval 3-6
set cdp hold-time 3-6
clear cdp 3-7
Cisco Discovery Protocol 3-8
Purpose 3-8
Commands 3-8
show ciscodp 3-8
show ciscodp port info 3-9
set ciscodp status 3-10
set ciscodp timer 3-11
set ciscodp holdtime 3-11
set ciscodp port 3-12
clear ciscodp 3-13
Link Layer Discovery Protocol and LLDP-MED 3-15
LLDP Frames 3-15
Configuration Tasks 3-15
Commands 3-16
show lldp 3-17
show lldp port status 3-18
show lldp port trap 3-18
show lldp port tx-tlv 3-19
show lldp port location-info 3-20
show lldp port local-info 3-20
show lldp port remote-info 3-23
show lldp port network-policy 3-24
set lldp tx-interval 3-26
set lldp hold-multiplier 3-26
set lldp trap-interval 3-27
set lldp med-fast-repeat 3-27
set lldp port status 3-28
set lldp port trap 3-29
set lldp port med-trap 3-29
set lldp port location-info 3-30
set lldp port tx-tlv 3-30
set lldp port network-policy 3-32
clear lldp 3-34
clear lldp port status 3-34

Downloaded from www.Manualslib.com manuals search engine

clear lldp port trap 3-35
clear lldp port med-trap 3-35
clear lldp port location-info 3-36
clear lldp port network-policy 3-36
clear lldp port tx-tlv 3-37

Chapter 4: Port Configuration

Port Configuration Summary 4-1
Port String Syntax Used in the CLI 4-2
Setting Console Port Properties 4-3
Purpose 4-3
Commands 4-3
show console 4-4
clear console 4-4
show console baud 4-5
set console baud 4-5
clear console baud 4-6
show console flowcontrol 4-6
set console flowcontrol 4-7
clear console flowcontrol 4-7
show console bits 4-8
set console bits 4-8
clear console bits 4-9
show console stopbits 4-9
set console stopbits 4-10
clear console stopbits 4-10
show console parity 4-11
set console parity 4-11
clear console parity 4-12
Reviewing Port Status 4-13
Purpose 4-13
Commands 4-13
show port 4-13
show port status 4-14
show port counters 4-15
show port operstatuscause 4-17
clear port operstatuscause 4-18
Disabling / Enabling and Naming Ports 4-20
Purpose 4-20
Commands 4-20
set port disable 4-20
set port enable 4-21
show port alias 4-21
set port alias 4-22
show forcelinkdown 4-22
set forcelinkdown 4-23
clear forcelinkdown 4-23
Setting Speed and Duplex Mode 4-24
Purpose 4-24
Commands 4-24
show port speed 4-24
set port speed 4-25
show port duplex 4-25
set port duplex 4-26
Enabling / Disabling Jumbo Frame Support 4-27

Downloaded from www.Manualslib.com manuals search engine

Purpose 4-27
Commands 4-27
show port jumbo 4-27
set port jumbo 4-28
clear port jumbo 4-28
Setting Auto-Negotiation and Advertised Ability 4-30
Purpose 4-30
Commands 4-30
show port negotiation 4-30
set port negotiation 4-31
show port mdix 4-31
set port mdix 4-32
clear port mdix 4-33
show port advertise 4-33
set port advertise 4-34
clear port advertise 4-35
Setting Flow Control 4-37
Purpose 4-37
Commands 4-37
show port flowcontrol 4-37
set port flowcontrol 4-38
Configuring Link Traps and Link Flap Detection 4-39
Purpose 4-39
Commands 4-39
show port trap 4-39
set port trap 4-40
show linkflap 4-40
set linkflap globalstate 4-43
set linkflap 4-43
set linkflap interval 4-44
set linkflap action 4-44
clear linkflap action 4-45
set linkflap threshold 4-45
set linkflap downtime 4-46
clear linkflap down 4-47
clear linkflap 4-47
Configuring Broadcast Suppression 4-49
Purpose 4-49
Commands 4-49
show port broadcast 4-49
set port broadcast 4-50
clear port broadcast 4-50
Configuring Port Mirroring 4-52
Supported Mirrors 4-52
Active Destination Port Configurations 4-52
Purpose 4-52
Commands 4-52
show port mirroring 4-52
set port mirroring 4-53
clear port mirroring 4-54
Configuring LACP 4-55
LACP Operation 4-55
LACP Terminology 4-56
Matrix Series Usage Considerations 4-56
Purpose 4-57
Commands 4-57

Downloaded from www.Manualslib.com manuals search engine

show lacp 4-58
set lacp 4-59
clear lacp state 4-60
set lacp asyspri 4-60
set lacp aadminkey 4-61
clear lacp 4-61
set lacp static 4-62
clear lacp static 4-63
show lacp singleportlag 4-63
set singleportlag 4-64
clear singleportlag 4-64
show port lacp 4-65
set port lacp 4-66
clear port lacp 4-68
show lacp flowRegeneration 4-69
set lacp flowRegeneration 4-69
clear lacp flowRegeneration 4-70
show lacp outportAlgorithm 4-70
set lacp outportAlgorithm 4-71
clear lacp outportAlgorithm 4-71

Chapter 5: SNMP Configuration

SNMP Configuration Summary 5-1
SNMPv1 and SNMPv2c 5-2
SNMPv3 5-2
About SNMP Security Models and Levels 5-2
Using SNMP Contexts to Access Specific MIBs 5-3
Creating a Basic SNMP Trap Configuration 5-3
Reviewing SNMP Statistics 5-5
Purpose 5-5
Commands 5-5
show snmp engineid 5-5
show snmp counters 5-6
Configuring SNMP Users, Groups and Communities 5-10
Purpose 5-10
Commands 5-10
show snmp user 5-10
set snmp user 5-12
clear snmp user 5-12
show snmp group 5-13
set snmp group 5-14
clear snmp group 5-15
show snmp community 5-15
set snmp community 5-16
clear snmp community 5-17
Configuring SNMP Access Rights 5-18
Purpose 5-18
Commands 5-18
show snmp access 5-18
set snmp access 5-20
clear snmp access 5-21
Configuring SNMP MIB Views 5-22
Purpose 5-22
Commands 5-22
show snmp view 5-22

Downloaded from www.Manualslib.com manuals search engine

show snmp context 5-23
set snmp view 5-24
clear snmp view 5-25
Configuring SNMP Target Parameters 5-26
Purpose 5-26
Commands 5-26
show snmp targetparams 5-26
set snmp targetparams 5-27
clear snmp targetparams 5-28
Configuring SNMP Target Addresses 5-29
Purpose 5-29
Commands 5-29
show snmp targetaddr 5-29
set snmp targetaddr 5-30
clear snmp targetaddr 5-31
Configuring SNMP Notification Parameters 5-33
Purpose 5-33
Commands 5-33
show snmp notify 5-33
set snmp notify 5-35
clear snmp notify 5-35
show snmp notifyfilter 5-36
set snmp notifyfilter 5-37
clear snmp notifyfilter 5-37
show snmp notifyprofile 5-38
set snmp notifyprofile 5-39
clear snmp notifyprofile 5-39
Configuring SNMP Walk Behavior 5-41
Purpose 5-41
Commands 5-41
set snmp timefilter break 5-41

Chapter 6: Spanning Tree Configuration

Overview: Single, Rapid and Multiple Spanning Tree Protocols 6-1
Spanning Tree Features 6-2
Loop Protect 6-2
Configuring Spanning Tree Bridge Parameters 6-3
Purpose 6-3
Commands 6-3
show spantree stats 6-6
show spantree version 6-9
set spantree version 6-9
clear spantree version 6-10
show spantree stpmode 6-10
set spantree stpmode 6-11
clear spantree stpmode 6-11
show spantree maxconfigurablestps 6-12
set spantree maxconfigurablestps 6-12
clear spantree maxconfigurablestps 6-13
show spantree mstilist 6-13
set spantree msti 6-14
clear spantree msti 6-14
show spantree mstmap 6-15
set spantree mstmap 6-15
clear spantree mstmap 6-16

Downloaded from www.Manualslib.com manuals search engine

show spantree vlanlist 6-16
show spantree mstcfgid 6-17
set spantree mstcfgid 6-17
clear spantree mstcfgid 6-18
show spantree bridgeprioritymode 6-18
set spantree bridgeprioritymode 6-19
clear spantree bridgeprioritymode 6-19
show spantree priority 6-20
set spantree priority 6-20
clear spantree priority 6-22
show spantree bridgehellomode 6-22
set spantree bridgehellomode 6-23
clear spantree bridgehellomode 6-23
show spantree hello 6-24
set spantree hello 6-24
clear spantree hello 6-25
show spantree maxage 6-25
set spantree maxage 6-26
clear spantree maxage 6-26
show spantree fwddelay 6-27
set spantree fwddelay 6-27
clear spantree fwddelay 6-28
show spantree autoedge 6-28
set spantree autoedge 6-29
clear spantree autoedge 6-29
show spantree legacypathcost 6-30
set spantree legacypathcost 6-30
clear spantree legacypathcost 6-31
show spantree tctrapsuppress 6-31
set spantree tctrapsuppress 6-32
clear spantree tctrapsuppress 6-32
show spantree txholdcount 6-33
set spantree txholdcount 6-33
clear spantree txholdcount 6-34
show spantree maxhops 6-34
set spantree maxhops 6-35
clear spantree maxhops 6-35
show spantree spanguard 6-36
set spantree spanguard 6-36
clear spantree spanguard 6-37
show spantree spanguardtimeout 6-37
set spantree spanguardtimeout 6-38
clear spantree spanguardtimeout 6-38
show spantree spanguardlock 6-39
clear / set spantree spanguardlock 6-39
show spantree spanguardtrapenable 6-40
set spantree spanguardtrapenable 6-40
clear spantree spanguardtrap enable 6-41
show spantree backuproot 6-41
set spantree backuproot 6-42
clear spantree backuproot 6-42
show spantree backuproottrapendable 6-43
set spantree backuproottrapenable 6-43
clear spantree backuproottrapenable 6-44
show spantree newroottrapendable 6-44
set spantree newroottrapenable 6-45

Downloaded from www.Manualslib.com manuals search engine

clear spantree newroottrapenable 6-45
clear spantree default 6-46
show spantree debug 6-46
clear spantree debug 6-48
Configuring Spanning Tree Port Parameters 6-49
Purpose 6-49
Commands 6-49
show spantree portenable 6-50
set spantree portenable 6-50
clear spantree portenable 6-51
show spantree portadmin 6-51
set spantree portadmin 6-52
clear spantree portadmin 6-52
set spantree protomigration 6-53
show spantree portstate 6-53
show spantree blockedports 6-54
show spantree portpri 6-54
set spantree portpri 6-55
clear spantree portpri 6-56
set spantree porthello 6-56
clear spantree porthello 6-57
show spantree portcost 6-57
show spantree adminpathcost 6-58
set spantree adminpathcost 6-58
clear spantree adminpathcost 6-59
show spantree adminedge 6-60
set spantree adminedge 6-60
clear spantree adminedge 6-61
show spantree operedge 6-61
show spantree adminpoint 6-62
show spantree operpoint 6-62
set spantree adminpoint 6-63
clear spantree adminpoint 6-64
Configuring Spanning Tree Loop Protect Features 6-65
Purpose 6-65
Commands 6-65
set spantree lp 6-65
show spantree lp 6-66
clear spantree lp 6-67
show spantree lplock 6-67
clear spantree lplock 6-68
set spantree lpcapablepartner 6-69
show spantree lpcapablepartner 6-70
clear spantree lpcapablepartner 6-70
set spantree lpthreshold 6-71
show spantree lpthreshold 6-71
clear spantree lpthreshold 6-72
set spantree lpwindow 6-72
show spantree lpwindow 6-73
clear spantree lpwindow 6-73
set spantree lptrapenable 6-74
show spantree lptrapenable 6-74
clear spantree lptrapenable 6-75
set spantree disputedbpduthreshold 6-75
show spantree disputedbpduthreshold 6-76
clear spantree disputedbpduthreshold 6-76

Downloaded from www.Manualslib.com manuals search engine

show spantree nonforwardingreason 6-77

Chapter 7: 802.1Q VLAN Configuration

VLAN Configuration Summary 7-1
Port Assignment Scheme 7-2
Port String Syntax Used in the CLI 7-2
Preparing for VLAN Configuration 7-2
About PVIDs and Policy Classification to a VLAN 7-2
Creating a Secure Management VLAN 7-2
Reviewing Existing VLANs 7-3
Purpose 7-3
Command 7-3
show vlan 7-3
Creating and Naming Static VLANs 7-6
Purpose 7-6
Commands 7-6
set vlan 7-6
set vlan name 7-7
clear vlan 7-7
clear vlan name 7-8
Assigning Port VLAN IDs (PVIDs) and Ingress Filtering 7-9
Purpose 7-9
Commands 7-9
show port vlan 7-9
set port vlan 7-10
clear port vlan 7-11
show vlan interface 7-11
set vlan interface 7-12
clear vlan interface 7-13
show port ingress filter 7-13
set port ingress filter 7-14
show port discard 7-15
set port discard 7-15
clear port discard 7-16
Configuring the VLAN Egress List 7-17
Purpose 7-17
Commands 7-17
show port egress 7-17
set vlan egress 7-18
clear vlan egress 7-19
show vlan dynamic egress 7-20
set vlan dynamicegress 7-20
Enabling/Disabling GVRP 7-22
Purpose 7-22
Commands 7-23
show gvrp 7-24
show garp timer 7-24
set gvrp 7-26
clear gvrp 7-26
set garp timer 7-27
clear garp timer 7-27

Chapter 8: Policy Classification Configuration

Policy Classification Configuration Summary 8-1
Configuring Policy Profiles 8-2

Downloaded from www.Manualslib.com manuals search engine

Purpose 8-2
Commands 8-2
show policy profile 8-2
set policy profile 8-3
clear policy profile 8-5
show policy invalid 8-5
set policy invalid action 8-6
clear policy invalid action 8-6
Assigning Classification Rules to Policy Profiles 8-7
Purpose 8-7
Commands 8-7
show policy rule 8-7
show policy capability 8-10
set policy classify 8-11
set policy rule 8-13
clear policy rule 8-15
clear policy all-rules 8-16
set policy port 8-17
show policy allowed-type 8-17
set policy allowed-type 8-18
clear policy allowed-type 8-19
clear policy port-hit 8-19
Configuring Policy Class of Service (CoS) 8-21
Using Port-Based or Policy-Based CoS Settings 8-21
About Policy-Based CoS Default and User-Defined Configurations 8-21
Purpose 8-22
Commands 8-22
show cos state 8-23
set cos state 8-23
show cos port-type 8-24
show cos unit 8-26
show cos port-config 8-27
set cos port-config irl 8-28
clear cos port-config irl 8-29
set cos port-config txq 8-29
clear cos port-config txq 8-30
show cos port-resource 8-31
set cos port-resource irl 8-32
clear cos port-resource irl 8-33
set cos port-resource txq 8-33
clear cos port-resource txq 8-34
show cos reference 8-35
set cos reference irl 8-36
clear cos reference irl 8-36
set cos reference txq 8-37
clear cos reference txq 8-37
show cos settings 8-38
set cos settings 8-39
clear cos settings 8-39
show cos violation irl 8-40
clear cos violation irl 8-40
clear cos all-entries 8-41
Configuring Policy-Based Routing 8-42
About Policy-Based Routing 8-42
Purpose 8-42
Commands 8-42

Downloaded from www.Manualslib.com manuals search engine

show route-map 8-42
route-map 8-43
match ip address 8-44
set next hop 8-45
show ip policy 8-45
ip policy route-map 8-46
ip policy priority 8-47
ip policy load-policy 8-48
ip policy pinger 8-48

Chapter 9: IGMP Configuration

About IP Multicast Group Management 9-1
IGMP Configuration Summary 9-2
Enabling / Disabling IGMP 9-2
Purpose 9-2
Commands 9-2
show igmp enable 9-2
set igmp enable 9-3
set igmp disable 9-3
Configuring IGMP 9-5
Purpose 9-5
Commands 9-5
show igmp query 9-5
set igmp query-enable 9-6
set igmp query-disable 9-6
show igmp grp-full-action 9-7
set igmp grp-full-action 9-7
show igmp config 9-8
set igmp config 9-9
set igmp delete 9-10
show igmp groups 9-10
show igmp static 9-11
set igmp add-static 9-11
set igmp remove-static 9-12
show igmp protocols 9-13
set igmp protocols 9-13
clear igmp protocols 9-14
show igmp vlan 9-14
show igmp reporters 9-15
show igmp flows 9-16
show igmp counters 9-16
show igmp number-groups 9-17

Chapter 10: System Logging Configuration

Configuring System Logging 10-1
Purpose 10-1
Commands 10-1
show logging all 10-2
show logging server 10-3
set logging server 10-4
clear logging server 10-5
show logging default 10-5
set logging default 10-6
clear logging default 10-7
show logging application 10-7

Downloaded from www.Manualslib.com manuals search engine

set logging application 10-9
clear logging application 10-11
show logging local 10-11
set logging local 10-12
clear logging local 10-12
set logging here 10-13
clear logging here 10-13
show logging buffer 10-14

Chapter 11: Network Monitoring Configuration

Monitoring Network Events and Status 11-1
Purpose 11-1
Commands 11-1
history 11-1
show history 11-2
set history 11-3
show netstat 11-3
ping 11-4
show users 11-6
tell 11-6
disconnect 11-7
Configuring SMON 11-8
Purpose 11-8
Commands 11-8
show smon priority 11-8
set smon priority 11-9
clear smon priority 11-9
show smon vlan 11-10
set smon vlan 11-11
clear smon vlan 11-11
Configuring RMON 11-13
RMON Monitoring Group Functions and Commands 11-13
show rmon stats 11-15
set rmon stats 11-17
clear rmon stats 11-17
show rmon history 11-18
set rmon history 11-19
clear rmon history 11-19
show rmon alarm 11-20
set rmon alarm properties 11-21
set rmon alarm status 11-22
clear rmon alarm 11-23
show rmon event 11-24
set rmon event properties 11-25
set rmon event status 11-25
clear rmon event 11-26
show rmon host 11-27
set rmon host properties 11-28
set rmon host status 11-28
clear rmon host 11-29
show rmon topN 11-29
set rmon topN properties 11-31
set rmon topN status 11-31
clear rmon topN 11-32
show rmon matrix 11-32

Downloaded from www.Manualslib.com manuals search engine

set rmon matrix properties 11-34
set rmon matrix status 11-34
clear rmon matrix 11-35
show rmon channel 11-35
set rmon channel 11-36
clear rmon channel 11-37
show rmon filter 11-37
set rmon filter 11-38
clear rmon filter 11-39
show rmon capture 11-40
set rmon capture 11-41
clear rmon capture 11-42

Chapter 12: Network Address and Route Management Configuration

Managing Switch Network Addresses and Routes 12-1
Purpose 12-1
Commands 12-1
show arp 12-2
set arp 12-3
clear arp 12-3
show rad 12-4
set rad 12-4
show ip route 12-5
traceroute 12-6
set ip route 12-8
clear ip route 12-8
show port mac 12-9
show mac 12-10
set mac 12-11
clear mac 12-12
show newaddrtraps 12-13
set newaddrtraps 12-14
show movedaddrtrap 12-14
set movedaddrtrap 12-15

Chapter 13: SNTP Configuration

Configuring Simple Network Time Protocol (SNTP) 13-1
Purpose 13-1
Commands 13-1
show sntp 13-2
set sntp client 13-3
clear sntp client 13-4
set sntp server 13-4
clear sntp server 13-5
set sntp broadcastdelay 13-5
clear sntp broadcast delay 13-6
set sntp poll-interval 13-6
clear sntp poll-interval 13-7
set sntp poll-retry 13-7
clear sntp poll-retry 13-7
set sntp poll-timeout 13-8
clear sntp poll-timeout 13-8
show timezone 13-9
set timezone 13-9
clear timezone 13-10

Downloaded from www.Manualslib.com manuals search engine

Chapter 14: Node Alias Configuration

Configuring Node Aliases 14-1
Purpose 14-1
Commands 14-1
show nodealias 14-1
show nodealias mac 14-2
show nodealias protocol 14-4
show nodealias config 14-5
set nodealias 14-6
set nodealias maxentries 14-7
clear nodealias 14-7
clear nodealias config 14-8

Chapter 15: NetFlow Configuration

Configuring NetFlow 15-1
Enterasys Matrix DFE Implementation 15-1
Operation 15-1
Version Support 15-2
Commands 15-2
show netflow 15-3
set netflow cache 15-4
clear netflow cache 15-4
set netflow export-destination 15-5
clear netflow export-destination 15-5
set netflow export-interval 15-6
clear netflow export-interval 15-7
set netflow port 15-7
clear netflow port 15-8
set netflow export-version 15-8
clear netflow export-version 15-9
set netflow template 15-9
clear netflow template 15-11

Chapter 16: IP Configuration

Configuring Routing Interface Settings 16-1
About Loopback Versus VLAN Interfaces 16-1
Purpose 16-2
Commands 16-2
show interface 16-2
interface 16-3
ip ecm-forwarding-algorithm 16-4
show ip interface 16-5
ip address 16-6
no shutdown 16-7
Managing Router Configuration Files 16-8
Purpose 16-8
Commands 16-8
show running-config 16-8
write 16-9
no ip routing 16-10
Performing a Basic Router Configuration 16-11
Using Router-Only Config Files 16-11
Displaying or Writing the Current Config to a File 16-11
Configuring the Router 16-11
Moving a Config File from Another Routing Module 16-11

Downloaded from www.Manualslib.com manuals search engine

Reviewing and Configuring the ARP Table 16-12
Purpose 16-12
Commands 16-12
show ip arp 16-12
arp 16-14
ip gratuitous-arp 16-15
ip gratuitous-arp-learning 16-15
ip proxy-arp 16-16
ip mac-address 16-17
arp timeout 16-17
clear arp-cache 16-18
Configuring Broadcast Settings 16-19
Applying DHCP/BOOTP Relay 16-19
Purpose 16-19
Commands 16-19
ip directed-broadcast 16-19
ip forward-protocol 16-20
ip helper-address 16-21
Reviewing IP Traffic and Configuring Routes 16-22
Purpose 16-22
Commands 16-22
show ip protocols 16-22
show ip traffic 16-23
clear ip stats 16-24
show ip route 16-25
ip route 16-26
ip icmp 16-27
ping 16-28
traceroute 16-28
Configuring Debug IP Packet 16-30
Purpose 16-30
Commands 16-30
debug ip packet access-group 16-30
debug ip packet restart 16-31
show debugging 16-32
no debug ip packet 16-32

Chapter 17: PIM Configuration

Configuring PIM 17-1
Purpose 17-1
Commands 17-1
ip pim sparse mode 17-2
ip pim bsr-candidate 17-2
ip pim dr-priority 17-3
ip pim rp-address 17-4
ip pim rp-candidate 17-5
show ip pim bsr 17-5
show ip pim interface 17-6
show ip pim neighbor 17-7
show ip pim rp 17-8
show ip pim rp-hash 17-10
show ip mroute 17-10
show ip mforward 17-11
show ip rpf 17-12

Downloaded from www.Manualslib.com manuals search engine

Chapter 18: Network Address Translation (NAT) Configuration

Configuring Network Address Translation (NAT) 18-1
NAT Configuration Task List and Commands 18-2
ip nat 18-3
ip nat pool 18-3
ip nat inside source list 18-4
ip nat inside source static (NAT) 18-5
ip nat inside source static (NAPT) 18-6
ip nat ftp-control-port 18-6
ip nat secure-plus 18-7
ip nat translation max-entries 18-8
ip nat translation (timeouts) 18-8
show ip nat translations 18-9
show ip nat statistics 18-10
clear ip nat translation 18-12
clear ip nat translation inside (NAT) 18-12
clear ip nat translation inside (NAPT) 18-13
set router limits (NAT) 18-14
show router limits (NAT) 18-15
clear router limits (NAT) 18-16

Chapter 19: LSNAT Configuration

Configuring Load Sharing Network Address Translation (LSNAT) 19-1
About LSNAT 19-1
LSNAT Configuration Considerations 19-1
Session Persistence 19-2
Sticky Persistence Configuration Considerations 19-2
Configuring Direct Access to Real Servers 19-3
Service Verification 19-3
Application Content Verification (ACV) 19-4
LSNAT Configuration Task List and Commands 19-5
show ip slb serverfarms 19-6
ip slb ftpctrlport 19-7
ip slb serverfarm 19-8
real 19-8
predictor 19-9
sticky 19-10
show ip slb reals 19-10
inservice (real server) 19-13
faildetect (real server) 19-13
faildetect acv-command 19-15
faildetect acv-reply 19-16
faildetect acv-quit 19-16
faildetect read-till-index 19-17
maxconns 19-18
weight 19-18
show ip slb vservers 19-19
ip slb vserver 19-21
serverfarm (Virtual Server) 19-22
virtual 19-22
inservice (virtual server) 19-24
client 19-24
persistence level 19-25
allow accessservers 19-27
ip slb allowaccess_all 19-28

Downloaded from www.Manualslib.com manuals search engine

show ip slb conns 19-29
show ip slb stats 19-30
show ip slb sticky 19-31
clear ip slb 19-32
show router limits (LSNAT) 19-32
set router limits (LSNAT) 19-33
clear router limits (LSNAT) 19-34

Chapter 20: DHCP Configuration

DHCP Overview 20-1
Configuring DHCP 20-1
DHCP Supported Options 20-2
DHCP Command Modes 20-4
Commands 20-5
ip dhcp server 20-6
ip local pool 20-6
exclude 20-7
ip dhcp ping packets 20-8
ip dhcp ping timeout 20-8
ip dhcp pool 20-9
domain-name 20-9
dns-server 20-10
netbios-name-server 20-11
netbios-node-type 20-11
default-router 20-12
bootfile 20-13
next-server 20-13
option 20-14
lease 20-15
host 20-16
client-class 20-16
client-identifier 20-17
client-name 20-18
hardware-address 20-18
show ip dhcp binding 20-19
clear ip dhcp binding 20-20
show ip dhcp server statistics 20-20
clear ip dhcp server statistics 20-22

Chapter 21: Routing Protocol Configuration

Activating Advanced Routing Features 21-1
Configuring RIP 21-1
Purpose 21-1
RIP Configuration Task List and Commands 21-1
router rip 21-2
network 21-3
neighbor 21-4
distance 21-4
ip rip offset 21-5
timers 21-6
ip rip send version 21-7
ip rip receive version 21-7
key chain 21-8
key 21-9
key-string 21-9

Downloaded from www.Manualslib.com manuals search engine

accept-lifetime 21-10
send-lifetime 21-11
ip rip authentication keychain 21-12
ip rip authentication mode 21-13
no auto-summary 21-13
ip rip disable-triggered-updates 21-14
ip split-horizon poison 21-15
passive-interface 21-15
receive-interface 21-16
distribute-list 21-17
redistribute 21-17
Configuring OSPF 21-19
Understanding Graceful Restart 21-19
Purpose 21-20
OSPF Configuration Task List and Commands 21-21
router ospf 21-22
network 21-23
router id 21-24
ip ospf cost 21-24
ip ospf priority 21-25
timers spf 21-26
ip ospf retransmit-interval 21-26
ip ospf transmit-delay 21-27
ip ospf hello-interval 21-28
ip ospf dead-interval 21-28
ip ospf authentication-key 21-29
ip ospf message digest key md5 21-30
distance ospf 21-30
area range 21-31
area authentication 21-32
area stub 21-33
area default cost 21-34
area nssa 21-34
area virtual-link 21-35
passive-interface 21-36
redistribute 21-37
database-overflow 21-38
graceful-restart enable 21-39
graceful-restart helper-disable 21-40
graceful-restart restart-interval 21-40
graceful-restart strict-lsa-checking-disable 21-41
show ip ospf 21-42
show ip ospf database 21-43
show ip ospf border-routers 21-45
show ip ospf interface 21-45
show ip ospf neighbor 21-47
show ip ospf virtual-links 21-48
clear ip ospf process 21-49
debug ip ospf 21-50
rfc1583compatible 21-50
Configuring DVMRP 21-52
Purpose 21-52
Commands 21-52
ip dvmrp 21-52
ip dvmrp metric 21-53
show ip dvmrp route 21-53

Downloaded from www.Manualslib.com manuals search engine

Configuring IRDP 21-55
Purpose 21-55
Commands 21-55
ip irdp 21-55
ip irdp maxadvertinterval 21-56
ip irdp minadvertinterval 21-56
ip irdp holdtime 21-57
ip irdp preference 21-58
ip irdp address 21-58
no ip irdp multicast 21-59
show ip irdp 21-59
Configuring VRRP 21-61
Purpose 21-61
Commands 21-61
router vrrp 21-61
create 21-62
address 21-63
priority 21-64
master-icmp-reply 21-65
advertise-interval 21-66
critical-ip 21-66
preempt 21-67
preempt-delay 21-68
enable 21-69
ip vrrp authentication-key 21-70
ip vrrp message-digest-key 21-70
show ip vrrp 21-71

Chapter 22: Port Priority and Rate Limiting Configuration

Port Priority Configuration Summary 22-1
Configuring Port Priority 22-2
Purpose 22-2
Commands 22-2
show port priority 22-2
set port priority 22-3
clear port priority 22-3
Configuring Priority to Transmit Queue Mapping 22-5
Purpose 22-5
Commands 22-5
show port priority-queue 22-5
set port priority-queue 22-6
clear port priority-queue 22-7
Configuring Port Traffic Rate Limiting 22-9
Purpose 22-9
Commands 22-9
show port ratelimit 22-9
set port ratelimit 22-10
clear port ratelimit 22-11

Chapter 23: Transparent Web Cache Balancing Configuration

Understanding Transparent Web Cache Balancing (TWCB) 23-1
Purpose 23-2
Commands 23-2
ip twcb wcserverfarm 23-3
predictor roundrobin 23-4

Downloaded from www.Manualslib.com manuals search engine

cache 23-5
faildetect type 23-5
faildetect 23-6
maxconns 23-7
inservice 23-7
ip twcb webcache 23-8
http-port 23-9
serverfarm 23-9
bypass-list range 23-10
hosts redirect range 23-10
ip twcb redirect out 23-11
show ip twcb wcserverfarm 23-12
show ip twcb webcache 23-13
show ip twcb conns 23-13
show ip twcb stats 23-14
clear ip twcb statistics 23-14
show limits 23-15
set router limits (TWCB) 23-15
show router limits (TWCB) 23-16
clear router limits (TWCB) 23-17
TWCB Configuration Example 23-19
Configure the s1Server Server Farm 23-19
Configure the s2Server Server Farm 23-20
Configure the cache1 Web Cache 23-21
Configure the Switch and Router 23-21

Chapter 24: Security Configuration

Overview of Security Methods 24-1
Configuring MAC Locking 24-2
Purpose 24-2
Commands 24-2
show maclock 24-2
show maclock stations 24-4
set maclock enable 24-5
set maclock disable 24-5
set maclock 24-6
set maclock firstarrival 24-7
set maclock move 24-7
clear maclock firstarrival 24-8
set maclock static 24-8
clear maclock static 24-9
set maclock trap 24-9
clear maclock 24-10
Configuring Secure Shell (SSH) 24-11
Purpose 24-11
Commands 24-11
show ssh state 24-11
set ssh 24-11
set ssh hostkey 24-12
show router ssh 24-12
set router ssh 24-13
clear router ssh 24-13
Configuring Access Lists 24-15
Purpose 24-15
Commands 24-15

Downloaded from www.Manualslib.com manuals search engine

show access-lists 24-15
access-list (standard) 24-16
access-list (extended) 24-17
ip access-group 24-20
Configuring Denial of Service (DoS) Prevention 24-22
Purpose 24-22
Commands 24-22
show hostdos 24-22
hostdos 24-23
clear hostdos-counters 24-24
Configuring Flow Setup Throttling (FST) 24-25
About FST 24-25
Purpose 24-25
Commands 24-25
show flowlimit 24-26
set flowlimit 24-26
set flowlimit limit 24-27
clear flowlimit limit 24-28
set flowlimit action 24-28
clear flowlimit action 24-29
show flowlimit class 24-30
set flowlimit port 24-31
clear flowlimit port class 24-32
set flowlimit shutdown 24-32
set flowlimit notification 24-33
clear flowlimit notification interval 24-34
clear flowlimit stats 24-34

Chapter 25: Authentication Configuration

Overview of Authentication Methods 25-1
Configuring 802.1X Authentication 25-2
About Multi-User Authentication 25-2
Purpose 25-2
Commands 25-3
show dot1x 25-3
show dot1x auth-config 25-5
set dot1x 25-7
set dot1x auth-config 25-7
clear dot1x auth-config 25-9
Configuring Port Web Authentication (PWA) 25-11
About PWA 25-11
Purpose 25-12
Commands 25-12
show pwa 25-13
set pwa 25-15
set pwa hostname 25-15
clear pwa hostname 25-16
show pwa banner 25-16
set pwa banner 25-17
set pwa displaylogo hide 25-17
clear pwa banner 25-17
set pwa displaylogo 25-18
set pwa redirecttime 25-18
set pwa ipaddress 25-19
set pwa protocol 25-19

Downloaded from www.Manualslib.com manuals search engine

set pwa enhancedmode 25-20
set pwa guestname 25-21
clear pwa guestname 25-21
set pwa guestpassword 25-22
set pwa gueststatus 25-22
set pwa initialize 25-23
set pwa quietperiod 25-23
set pwa maxrequests 25-24
set pwa portcontrol 25-24
show pwa session 25-25
Configuring MAC Authentication 25-26
Purpose 25-26
Commands 25-26
show macauthentication 25-26
show macauthentication session 25-28
set macauthentication 25-29
set macauthentication password 25-29
clear macauthentication password 25-30
set macauthentication significant-bits 25-30
clear macauthentication significant-bits 25-31
set macauthentication port 25-31
set macauthentication authallocated 25-32
clear macauthentication authallocated 25-32
set macauthentication portinitialize 25-33
set macauthentication macinitialize 25-33
set macauthentication reauthentication 25-34
set macauthentication portreauthenticate 25-34
set macauthentication macreauthenticate 25-35
set macauthentication reauthperiod 25-35
clear macauthentication reauthperiod 25-36
set macauthentication quietperiod 25-37
clear macauthentication quietperiod 25-37
Configuring Convergence End Points (CEP) Phone Detection 25-39
About CEP Phone Detection 25-39
Purpose 25-39
Commands 25-39
show cep connections 25-40
show cep detection 25-40
show cep policy 25-41
show cep port 25-42
set cep 25-42
set cep port 25-43
set cep policy 25-43
set cep detection-id 25-44
set cep detection-id type 25-45
set cep detection-id address 25-46
set cep detection-id protocol 25-46
set cep detection-id porthigh | portlow 25-47
set cep initialize 25-48
clear cep 25-49
RADIUS Filter-ID Attribute and Dynamic Policy Profile Assignment 25-50
Filter-ID Attribute Formats 25-50
Setting the Authentication Login Method 25-50
Purpose 25-50
Commands 25-50
show authentication login 25-51

Downloaded from www.Manualslib.com manuals search engine

set authentication login 25-51
clear authentication login 25-52
Configuring RADIUS 25-53
Purpose 25-53
Commands 25-53
show radius 25-53
set radius 25-54
clear radius 25-55
show radius accounting 25-56
set radius accounting 25-57
clear radius accounting 25-58
Configuring RFC 3580 25-60
About RFC 3580 25-60
Purpose 25-60
Commands 25-60
show vlanauthorization 25-60
set vlanauthorization 25-61
clear vlanauthorization 25-62
Configuring TACACS+ 25-63
Purpose 25-63
Commands 25-63
show tacacs 25-63
set tacacs 25-65
show tacacs server 25-65
set tacacs server 25-66
clear tacacs server 25-67
show tacacs session 25-67
set tacacs session 25-68
clear tacacs session 25-69
show tacacs command 25-70
set tacacs command 25-71
show tacacs singleconnect 25-71
set tacacs singleconnect 25-72

Chapter 26: RADIUS Snooping Configuration

Understanding RADIUS Snooper 26-1
Purpose 26-2
Commands 26-2
set radius-snooping 26-2
set radius-snooping timeout 26-3
set radius-snooping port 26-4
set radius-snooping flow 26-5
set radius-snooping initialize 26-6
clear radius-snooping all 26-6
clear radius-snooping flow 26-7
show radius-snooping 26-7
show radius-snooping port 26-8
show radius-snooping flow 26-9
show radius-snooping session 26-10

Chapter 27: MultiAuth Configuration

Configuring Multiple Authentication 27-1
About Multiple Authentication 27-1
DFE-Gold Multi-User Capacities 27-1
set multiauth mode 27-2

Downloaded from www.Manualslib.com manuals search engine

clear multiauth mode 27-3
show multiauth 27-3
show multiauth counters 27-4
set multiauth precedence 27-5
clear multiauth precedence 27-5
show multiauth port 27-6
set multiauth port 27-6
clear multiauth port 27-7
show multiauth station 27-8
clear multiauth station 27-8
show multiauth session 27-9
show multiauth idle-timeout 27-10
set multiauth idle-timeout 27-10
clear multiauth idle-timeout 27-11
show multiauth session-timeout 27-12
set multiauth session-timeout 27-13
clear multiauth session-timeout 27-14
set multiauth trap 27-14
clear multiauth trap 27-15
show multiauth trap 27-16

Index

Figures

2-1 Matrix DFE-Gold Startup Screen 2-8
2-2 Performing a Keyword Lookup 2-9
2-3 Performing a Partial Keyword Lookup 2-10
2-4 Scrolling Screen Output 2-10
2-5 Abbreviating a Command 2-11
2-6 Completing a Partial Command 2-11
2-7 Basic Line Editing Emacs & vi Commands 2-11
2-8 Enabling the Switch for Routing 2-101
7-1 Example of VLAN Propagation via GVRP 7-23
16-1 Example of a Simple Enterasys Matrix Series Router Config File 16-11
21-1 Physical and Logical Single Router HA Failover Configuration 21-20
23-1 TWCB Configuration Overview 23-2
23-2 TWCB Configuration Example Overview 23-19

Tables

2-1 Default Device Settings for Basic Switch Operation 2-2
2-2 Default Device Settings for Router Mode Operation 2-5
2-3 show system login Output Details 2-16
2-4 show system lockout Output Details 2-24
2-5 Show System Output Display 2-35
2-6 show version Output Details 2-49
2-7 dir Output Details 2-82
2-8 Enabling the Switch for Routing 2-100
2-9 Router CLI Configuration Modes 2-103
3-1 show cdp Output Details 3-4
3-2 show ciscodp Output Details 3-9
3-3 show port ciscodp info Output Details 3-10
3-4 show lldp port local-info Output Details 3-21
3-5 show lldp port remote-info Output Display 3-24
4-1 show port status Output Details 4-14
4-2 show port counters Output Details 4-16

Downloaded from www.Manualslib.com manuals search engine

4-3 show port advertise Output Details 4-34
4-4 show port flow control Output Details 4-38
4-5 show linkflap parameters Output Details 4-42
4-6 show linkflap metrics Output Details 4-42
4-7 show port broadcast Output Details 4-50
4-8 LACP Terms and Definitions 4-56
4-9 show lacp Output Details 4-59
5-1 SNMP Security Levels 5-3
5-2 Basic SNMP Trap Configuration Command Set 5-4
5-3 show snmp engineid Output Details 5-6
5-4 show snmp counters Output Details 5-7
5-5 show snmp user Output Details 5-11
5-6 show snmp group Output Details 5-14
5-7 show snmp access Output Details 5-19
5-8 show snmp view Output Details 5-23
5-9 show snmp targetparams Output Details 5-27
5-10 show snmp targetaddr Output Details 5-30
5-11 show snmp notify Output Details 5-34
6-1 show spantree Output Details 6-7
6-2 Port-Specific show spantree stats Output Details 6-8
7-1 Command Set for Creating a Secure Management VLAN 7-3
7-2 show vlan Output Details 7-4
7-3 show vlan interface Output Details 7-12
7-4 show gvrp Output Details 7-24
7-5 show gvrp configuration Output Details 7-25
8-1 show policy profile Output Details 8-3
8-2 show policy rule Output Details 8-9
8-3 Valid Values for Policy Classification Rules 8-15
8-4 Configuring User-Defined CoS 8-21
8-5 show cos port-type Output Details 8-25
8-6 show ip policy Output Details 8-46
9-1 show igmp config Output Details 9-8
10-1 show logging all Output Details 10-3
10-2 show logging application Output Details 10-9
10-3 Sample Mnemonic Values for Logging Applications 10-10
11-1 show netstat Output Details 11-4
11-2 RMON Monitoring Group Functions and Commands 11-13
11-3 show rmon stats Output Details 11-16
11-4 show rmon alarm Output Details 11-21
11-5 show rmon event Output Details 11-24
11-6 show rmon topN Output Details 11-30
11-7 show rmon matrix Output Details 11-33
12-1 show arp Output Details 12-3
12-2 show ip route Output Details 12-6
12-3 show mac Output Details 12-11
13-1 show sntp Output Details 13-2
14-1 show nodealias Output Details 14-2
14-2 show nodealias config Output Details 14-6
16-1 VLAN and Loopback Interface Configuration Modes 16-2
16-2 show ip interface Output Details 16-5
16-3 show ip arp Output Details 16-14
17-1 show ip pim bsr Output Details 17-6
17-2 show ip pim interface Output Details 17-7
17-3 show ip pim neighbor Output Details 17-8
17-4 show ip pim rp Output Details 17-9
18-1 NAT Configuration Task List and Commands 18-2

Downloaded from www.Manualslib.com manuals search engine

19-1 LSNAT Configuration Task List and Commands 19-5
19-2 show ip slb reals Output Details 19-12
19-3 show ip slb vservers Output Details 19-20
19-4 show ip slb conns Output Details 19-30
20-1 DHCP Server Supported Options 20-2
20-2 DHCP Command Modes 20-4
20-3 show ip dhcp server statistics Output Details 20-21
21-1 RIP Configuration Task List and Commands 21-2
21-2 OSPF Configuration Task List and Commands 21-21
21-3 show ip ospf database Output Details 21-44
21-4 show ip ospf interface Output Details 21-46
21-5 show ip ospf neighbor Output Details 21-48
21-6 show ip ospf virtual links Output Details 21-49
21-7 show ip vrrp Output Details 21-72
22-1 show port ratelimit Output Details 22-10
24-1 show maclock Output Details 24-3
24-2 show maclock stations Output Details 24-4
25-1 show pwa Output Details 25-14
25-2 show macauthentication Output Details 25-27
25-3 show macauthentication session Output Details 25-29
25-4 show radius Output Details 25-54
25-5 show tacacs Output Details 25-64
26-1 Radius-Snooping Settings 26-8
26-2 Radius-Snooping Port Settings 26-9
26-3 Radius-Snooping Flow Settings 26-10
26-4 Radius-Snooping Session Port Settings 26-11
26-5 Radius-Snooping Session MAC Settings 26-11

Downloaded from www.Manualslib.com manuals search engine

About This Guide

This manual explains how to access the device's Command Line Interface (CLI) and how to use it to configure Enterasys Matrix® DFE-Gold Series switch/router devices.

Important Notice

Depending on the firmware version used in your Matrix Series device, some features described in this document may not be supported. Refer to the Release Notes shipped with your Matrix Series device to determine which features are supported.

Using This Guide

A general working knowledge of basic network operations and an understanding of CLI management applications is helpful before configuring the Matrix Series device.

This manual describes how to do the following:

- Access the Matrix Series CLI.
- Use CLI commands to perform network management and device configuration operations.
- Establish and manage Virtual Local Area Networks (VLANs).
- Manage static and dynamically-assigned user policies.
- Establish and manage priority classification.
- Configure IP routing and routing protocols, including RIP versions 1 and 2, OSPF, DVMRP, IRDP, and VRRP.
- Configure security protocols, including 802.1X and RADIUS, SSHv2, MAC locking, MAC authentication, multiple authentication, DoS attack prevention, and flow setup throttling.
- Configure policy-based routing.
- Configure access control lists (ACLs).

Structure of This Guide

The guide is organized as follows:

Chapter 1, **Introduction**, provides an overview of the tasks that can be accomplished using the CLI interface, an overview of local management requirements, and information about obtaining technical support.

Chapter 2, **Startup and General Configuration**, provides an overview of the device's factory default settings and describes how to start the CLI interface, how to set basic system properties, how to download a firmware image, how to configure WebView and Telnet, how to manage configuration files, how to set the login password, how to exit the CLI, and how to prepare the device for router mode operation.

Chapter 3, **Discovery Protocols Configuration**, describes how to configure the three discovery protocols supported by the firmware using CLI commands, including the Enterasys Discovery

Downloaded from www.Manualslib.com manuals search engine

Protocol, the Cisco Discovery Protocol, and the IEEE 802.1AB Link Layer Discovery Protocol (LLDP) and LLDP Media Endpoint Discovery Protcol (LLDP-MED).

Chapter 4, **Port Configuration**, describes how to review and configure console port settings, and how to enable or disable switch ports and configure switch port settings, including port speed, duplex mode, auto-negotiation, flow control, port mirroring, link aggegation and broadcast suppression.

Chapter 5, **SNMP Configuration**, describes how to configure SNMP users and user groups, access rights, target addresses, and notification parameters.

Chapter 6 **Spanning Tree Configuration**, describes how to review and set Spanning Tree bridge parameters for the device, including bridge priority, hello time, maximum aging time and forward delay; and how to review and set Spanning Tree port parameters, including port priority and path costs. Also describes how to configure the Loop Protect feature.

Chapter 7, **802.1Q VLAN Configuration**, describes how to create static VLANs, select the mode of operation for each port, establish VLAN forwarding (egress) lists, route frames according to VLAN ID, display the current ports and port types associated with a VLAN and protocol, create a secure management VLAN, and configure ports on the device as GVRP-aware ports.

Chapter 8, **Policy Classification Configuration**, describes how to create, change or remove user roles or profiles based on business-specific use of network services; how to permit or deny access to specific services by creating and assigning classification rules which map user profiles to frame filtering policies; how to classify frames to a VLAN or Class of Service (CoS); and how to assign or unassign ports to policy profiles so that only ports activated for a profile will be allowed to transmit frames accordingly.

Chapter 9, **IGMP Configuration**, describes how to configure Internet Group Management Protocol (IGMP) settings for multicast filtering, including IGMP query count, IGMP report delay and IGMP group status.

Chapter 10, **System Logging Configuration**, describes how to configure and display statistics for Syslog.

Chapter 11, **Network Monitoring Configuration**, describes how to manage general switch settings, how to monitor network events and status while the device is in switch mode, including the eventlog, command history, netstats and RMON statistics.

Chapter 12, **Network Address and Route Management Configuration**, describes how to manage network addresses and routes.

Chapter 13, **SNTP Configuration**, describes how to configure and display statistics for SNTP.

Chapter 14, **Node Alias Configuration**, describes how to configure and display statistics for node aliases.

Chapter 15, **NetFlow Configuration**, describes how to configure NetFlow cache, port template and related parameters.

Chapter 16, **IP Configuration**, describes how to enable IP routing for router mode operation, how to configure IP interface settings, how to review and configure the routing ARP table, how to review and configure routing broadcasts, how to configure PIM, how to configure LSNAT and DHCP server, and how to configure IP routes.

Chapter 17, **PIM Configuration**, describes how to configure and display statistics for Protocol Independent Multicast.

Chapter 18, **Network Address Translation (NAT) Configuration**, describes how to configure and display statistics for Network Address Translation.

Chapter 19, **LSNAT Configuration**, describes how to configure and display statistics for Load Sharing Network Address Translation.

Downloaded from www.Manualslib.com manuals search engine

Chapter 20, **DHCP Configuration**, describes how to configure and display statistics for Dynamic Host Configuration Protocol.

Chapter 21, **Routing Protocol Configuration**, describes how to configure RIP, OSPF, DVMRP, IRDP and VRRP.

Chapter 22, **Port Priority and Rate Limiting Configuration**, describes how to set the transmit priority of each port, display the current traffic class mapping-to-priority of each port, set ports to either transmit frames according to selected priority transmit queues or percentage of port transmission capacity for each queue, and configure a rate limit for a given port and list of priorities.

Chapter 23, **Transparent Web Cache Balancing Configuration**, describes how to configure and display statistics for Transparent Web Cache Balancing.

Chapter 24, **Security Configuration**, describes how to configure Secure Shell server, MAC locking, policy-based routing, and IP access control lists (ACLs), Denial of Service (DoS) prevention, and flow setup throttling.

Chapter 25, **Authentication Configuration**, describes how to configure 802.1X Network Access Control, Port Web Authentication (PWA), MAC Authentication, and Convergence End Point (CEP), RADIUS server, TACACS+, and RFC3580.

Chapter 26, **RADIUS Snooping Configuration**, describes how to configure and display statistics for the RADIUS Snooping authentication method.

Chapter 27, **MultiAuth Configuration**, describes how to configure Multi-Authentication.

Related Documents

The following Enterasys Networks documents may help you to set up, control, and manage the Matrix Series device:

- Matrix Series Installation Guide(s)
- Matrix WebView User's Guide
- A series of Enterasys feature guides that provide overviews of key switching and routing features of the Matrix DFE products, detailed descriptions of feature operation, and configuration examples.

Documents listed above, can be obtained from the World Wide Web in Adobe Acrobat Portable Document Format (PDF) at the following web site:

http://www.enterasys.com/support/manuals/

Downloaded from www.Manualslib.com manuals search engine

Conventions Used in This Guide

The following conventions are used in the text of this document:

Convention	Description
Bold font	Indicates mandatory keywords, parameters or keyboard keys.
italic font	Indicates complete document titles.
`Courier` font	Used for examples of information displayed on the screen.
`Courier` font in italics	Indicates a user-supplied value, either required or optional.
[ ]	Square brackets indicate an optional value.
{ }	Braces indicate required values. One or more values may be required.
|	A vertical bar indicates a choice in values.
[x | y | z]	Square brackets with a vertical bar indicates a choice of a value.
{x | y | z}	Braces with a vertical bar indicate a choice of a required value.
[x {y | z}]	A combination of square brackets with braces and vertical bars indicates a required choice of an optional value.

The following icons are used in this guide:



Note: Calls the reader's attention to any item of information that may be of special importance.



Router: Calls the reader's attention to router-specific commands and information.



Caution: Contains information essential to avoid damage to the equipment.

Precaución: Contiene información esencial para prevenir dañar el equipo.

Achtung: Verweißt auf wichtige Informationen zum Schutz gegen Beschädigungen.



Warning: Warns against an action that could result in personal injury or death.

Advertencia: Advierte contra una acción que pudiera resultar en lesión corporal o la muerte.

Warnhinweis: Warnung vor Handlungen, die zu Verletzung von Personen oder gar Todesfällen führen können!



Electrical Hazard: Warns against an action that could result in personal injury or death.

Riesgo Electrico: Advierte contra una acción que pudiera resultar en lesión corporal o la muerte debido a un riesgo eléctrico.

Elektrischer Gefahrenhinweis: Warnung vor sämtlichen Handlungen, die zu Verletzung von Personen oder Todesfällen – hervorgerufen durch elektrische Spannung – führen können!

Downloaded from www.Manualslib.com manuals search engine

Getting Help

For additional support related to the product or this document, contact Enterasys Networks using one of the following methods:

World Wide Web	www.enterasys.com/support
Phone	1-800-872-8440 (toll-free in U.S. and Canada) or 1-978-684-1000 To find the Enterasys Networks Support toll-free number in your country: www.enterasys.com/support
Internet mail	support@enterasys.com To expedite your message, type **[N-SERIES]** in the subject line.
To send comments concerning this document to the Technical Publications Department: techpubs@enterasys.com Please include the document Part Number in your email message.	

Before contacting Enterasys Networks for technical support, have the following information ready:

- Your Enterasys Networks service contract number
- A description of the failure
- A description of any action(s) already taken to resolve the problem (for example, changing mode switches or rebooting the unit)
- The serial and revision numbers of all involved Enterasys Networks products in the network
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load and frame size at the time of trouble (if known)
- The device history (for example, if you have returned the device before, or if this a recurring problem)
- Any previous Return Material Authorization (RMA) numbers

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

1

Introduction

This chapter provides an overview of the Enterasys Matrix Series' unique features and functionality, an overview of the tasks that may be accomplished using the CLI interface, an overview of ways to manage the device, and information on how to contact Enterasys Networks for technical support.

Matrix DFE Series Features

Matrix Series devices support business-driven networking with:

- New Enterasys advanced Distributed Forwarding Engine (DFE) architecture allowing for single IP address management of an entire chassis.
- High availability design featuring fully redundant, hot-swappable modules, power supplies and fans.
- Advanced QoS and policy-based frame classification, and bandwidth management featuring rate limiting, CoS priority queueing and link aggregation.
- Customized, single-source management and control with SNMP, port mirroring, Syslog, RMON, multi-image support and configuration upload/download.

Matrix Series CLI Overview

Enterasys Networks' Matrix Series CLI interface allows you to perform a variety of network management tasks, including the following:

- Assign IP address and subnet mask.
- Select a default gateway.
- Assign a login password to the device for additional security.
- Download a new firmware image.
- Designate which network management workstations receive SNMP traps from the device.
- View device, interface, and RMON statistics.
- Manage configuration files.
- Assign ports to operate in the standard or full duplex mode.
- Control the number of received broadcasts that are switched to the other interfaces.
- Set flow control on a port-by-port basis.
- Set port configurations and port-based VLANs.
- Configure ports to prioritize and assign a VLAN or Class of Service to incoming frames based on Layer 2, Layer 3, and Layer 4 information.

Downloaded from www.Manualslib.com manuals search engine

- Configure the device to operate as a Generic Attribute Registration Protocol (GARP) device to dynamically create VLANs across a switched network.
- Redirect frames according to a port or VLAN and transmit them on a preselected destination port.
- Configure Spanning Trees.
- Clear NVRAM.
- Configure interfaces for IP routing.
- Configure RIP, OSPF, DVMRP, IRDP and VRRP routing protocols.
- Configure security methods, including 802.1X. RADIUS, TACACS, CEP, SSHv2, MAC locking, and DoS attack prevention.
- Configure access lists (ACLs).

Device Management Methods

The Matrix Series device can be managed using the following methods:

- Locally using a VT type terminal connected to the console port.
- Remotely using a VT type terminal connected through a modem.
- Remotely using an SNMP management station.
- In-band through a Telnet connection.
- In-band using Enterasys Networks' NetSight® management application.
- Remotely using WebView™, Enterasys Networks' embedded web server application.

The *Enterasys Matrix Series Installation Guide* provides setup instructions for connecting a terminal or modem to the Matrix Series device.

Downloaded from www.Manualslib.com manuals search engine

2

Startup and General Configuration

This chapter describes factory default settings and the Startup and General Configuration set of commands.

For information about...	Refer to page...
Startup and General Configuration Summary	2-1
Setting User Accounts and Passwords	2-15
Managing the Management Authentication Notification MIB	2-26
Setting Basic Device Properties	2-30
Activating Licensed Features	2-58
Configuring Power over Ethernet (PoE)	2-61
Reviewing and Selecting a Boot Firmware Image	2-72
Starting and Configuring Telnet	2-76
Managing Configuration and Image Files	2-80
Enabling or Disabling the Path MTU Discovery Protocol	2-90
Pausing, Clearing and Closing the CLI	2-92
Resetting the Device	2-94
Gathering Technical Support Information	2-98
Preparing the Device for Router Mode	2-100
Reviewing and Configuring Routing	2-101

Startup and General Configuration Summary

At startup, the Matrix Series device is configured with many defaults and standard features. The following sections provide information on how to review and change factory defaults, how to customize basic system settings to adapt to your work environment, and how to prepare to run the device in router mode.

Factory Default Settings

The following tables list factory default device settings available on the Matrix Series device. Table 2-1 lists default settings for Matrix Series switch operation. Table 2-2 lists default settings for router mode operation.

Downloaded from www.Manualslib.com manuals search engine

Table 2-1 Default Device Settings for Basic Switch Operation

Device Feature	Default Setting
CDP discovery protocol	Auto enabled on all ports.
CDP authentication code	Set to **00-00-00-00-00-00-00-00**
CDP hold time	Set to **180** seconds.
CDP interval	Transmit frequency of CDP messages set to **60** seconds.
Cisco Discovery Protocol	Globally auto-enabled, enabled on ports.
Community name	Public.
Convergence End Points phone detection	Disabled globally and on all ports
EAPOL	Disabled.
EAPOL authentication mode	When enabled, set to **auto** for all ports.
GARP timer	Join timer set to **20** centiseconds; leave timer set to **60** centiseconds; leaveall timer set to **1000** centiseconds.
GVRP	Globally enabled.
IGMP	Disabled. When enabled, query interval is set to **125**seconds and response time is set to **100** tenths of a second.
IP mask and gateway	Subnet mask set to **255.0.0.0**; default gateway set to **0.0.0.0**
IP routes	No static routes configured.
Jumbo frame support	Disabled on all ports.
Link aggregation admin key	Set to 32768 for all ports.
Link aggregation flow regeneration	Disabled.
Link aggregation system priority	Set to 32768 for all ports.
Link aggregation outport algorithm	Set to DIP-SIP.
Link Layer Discovery Protocol (LLDP)	Both transmitting and receiving LLDPDUs are enabled.
LLDP transmit interval	30 seconds
LLDP hold multiplier	4
LLDP trap interval	5 seconds
LLDP-MED fast repeat	3 fast start LLDPDUs
LLDP traps	Disabled
LLDP-MED traps	Disabled
Lockout	Set to disable Read-Write and Read-Only users, and to lockout the default admin (Super User) account for 15 minutes, after 3 failed login attempts,
Logging	Syslog port set to UDP port number **514**. Logging severity level set to **6** (significant conditions) for all applications.

Downloaded from www.Manualslib.com manuals search engine

Table 2-1 Default Device Settings for Basic Switch Operation (continued)

Device Feature	Default Setting
MAC aging time	Set to 300 seconds.
MAC locking	Disabled (globally and on all ports).
Management Authentication Notification	Enabled
MTU discovery protocol	Enabled.
NetFlow collection	Disabled
NetFlow export version	Version 5
NetFlow Version 9 template refresh rate	20 packets
NetFlow Version 9 template timeout	30 minutes
Passwords	Set to an empty string for all default user accounts. User must press ENTER at the password prompt to access CLI.
Password aging	Disabled.
Password history	No passwords are checked for duplication.
Policy classification	Classification rules are automatically enabled when created.
Port auto-negotiation	Enabled on all ports.
Port advertised ability	Maximum ability advertised on all ports.
Port broadcast suppression	Disabled (no broadcast limit).
Port duplex mode	Set to **half** duplex, except for 100BASE-FX and 1000BASE-X, which is set to **full** duplex.
Port enable/disable	Enabled.
Port priority	Set to **1**.
Port speed	Set to **10** Mbps, except for 1000BASE-X, which is set to **1000** Mbps, and **100**BASE-FX, which is set to 100 Mbps.
Port trap	All ports are enabled to send link traps.
Priority classification	Classification rules are automatically enabled when created.
RADIUS client	Disabled.
RADIUS last resort action	When the client is enabled, set to **Challenge**.
RADIUS retries	When the client is enabled, set to **3**.
RADIUS timeout	When the client is enabled, set to **20** seconds.
Rate limiting	Disabled (globally and on all ports).
SNMP	Enabled.
SNTP	Disabled.
Spanning Tree	Globally enabled and enabled on all ports.
Spanning Tree edge port administrative status	Enabled.

Downloaded from www.Manualslib.com manuals search engine

Table 2-1 Default Device Settings for Basic Switch Operation (continued)

Device Feature	Default Setting
Spanning Tree edge port delay	Enabled.
Spanning Tree forward delay	Set to **15** seconds.
Spanning Tree hello interval	Set to **2** seconds.
Spanning Tree ID (SID)	Set to **0**.
Spanning Tree legacy path cost	Disabled.
Spanning Tree maximum aging time	Set to **20** seconds.
Spanning Tree point-to-point	Set to **auto** for all Spanning Tree ports.
Spanning Tree port priority	All ports with bridge priority are set to **128** (medium priority).
Spanning Tree priority	Bridge priority is set to **32768**.
Spanning Tree topology change trap suppression	Enabled.
Spanning Tree transmit hold count	Set to **3**.
Spanning Tree version	Set to **mstp** (Multiple Spanning Tree Protocol).
Spanning Tree Loop Protect	Disabled per port and per SID.
Spanning Tree Loop Protect event threshold	3 events.
Spanning Tree Loop Protect event window	180 seconds.
Spanning Tree Loop Protect traps	Disabled.
Spanning Tree disputed BPDU threshold	Set to 0, meaning no traps are sent.
SSH	Disabled.
System baud rate	Set to **9600** baud.
System contact	Set to empty string.
System location	Set to empty string.
System name	Set to empty string.
Terminal	CLI display set to **80** columns and **24** rows.
Timeout	Set to **15** minutes.
User names	Login accounts set to **ro** for Read-Only access; **rw** for Read-Write access; and **admin** for Super User access.
VLAN dynamic egress	Disabled on all VLANs.

Downloaded from www.Manualslib.com manuals search engine

Table 2-1 Default Device Settings for Basic Switch Operation (continued)

Device Feature	Default Setting
VLAN ID	All ports use a VLAN identifier of **1**.
WebView (HTTP)	Enabled on TCP port 80.

Table 2-2 Default Device Settings for Router Mode Operation

Device Feature	Default Setting
Access groups (IP security)	None configured.
Access lists (IP security)	None configured.
Area authentication (OSPF)	Disabled.
Area default cost (OSPF)	Set to **1**.
Area NSSA (OSPF)	None configured.
Area range (OSPF)	None configured.
ARP table	No permanent entries configured.
ARP timeout	Set to **14,400** seconds.
Authentication key (RIP and OSPF)	None configured.
Authentication mode (RIP and OSPF)	None configured.
Dead interval (OSPF)	Set to **40** seconds.
Disable triggered updates (RIP)	Triggered updates allowed.
Distribute list (RIP)	No filters applied.
DoS prevention	Disabled.
DVMRP	Disabled. Metric set to **1**.
Hello interval (OSPF)	Set to **10** seconds for broadcast and point-to-point networks. Set to **30** seconds for non-broadcast and point-to-multipoint networks.
ICMP	Enabled for echo-reply and mask-reply modes.
IP-directed broadcasts	Disabled.
IP forward-protocol	Enabled with no port specified.
IP interfaces	Disabled with no IP addresses specified.
IRDP	Disabled on all interfaces. When enabled, maximum advertisement interval is set to **600** seconds, minimum advertisement interval is set to **450** seconds, holdtime is set to **1800** seconds, and address preference is set to **0**.
MD5 authentication (OSPF)	Disabled with no password set.
MTU size	Set to **1500** bytes on all interfaces.
OSPF	Disabled.
OSPF cost	Set to **10** for all interfaces.
OSPF network	None configured.

Downloaded from www.Manualslib.com manuals search engine

Table 2-2 Default Device Settings for Router Mode Operation (continued)

Device Feature	Default Setting
OSPF priority	Set to **1**.
Passive interfaces (RIP)	None configured.
Proxy ARP	Enabled on all interfaces.
Receive interfaces (RIP)	Enabled on all interfaces.
Retransmit delay (OSPF)	Set to **1** second.
Retransmit interval (OSPF)	Set to **5** seconds.
RIP receive version	Set to accept both version **1** and version **2**.
RIP send version	Set to version **1**.
RIP offset	No value applied.
SNMP	Enabled.
Split horizon	Enabled for RIP packets without poison reverse.
Stub area (OSPF)	None configured.
Telnet	Enabled.
Telnet port (IP)	Set to port number **23**.
Timers (OSPF)	SPF delay set to **5** seconds. SPF holdtime set to **10** seconds.
Transmit delay (OSPF)	Set to **1** second.
VRRP	Disabled.

CLI "Defaults" Descriptions

Each command description in this guide includes a section entitled "Defaults" which contains different information than the factory default settings on the device as described in Table 2-1 and Table 2-2. The command defaults section defines CLI behavior if the user enters a command without typing optional parameters (indicated by square brackets [ ]). For commands without optional parameters, the defaults section lists "None". For commands with optional parameters, this section describes how the CLI responds if the user opts to enter only the keywords of the command syntax.

CLI Command Modes

Each command description in this guide includes a section entitled "Command Mode" which states whether the command is executable in Admin (Super User), Read-Write or Read-Only mode. Users with Read-Only access will only be permitted to view Read-Only (**show**) commands. Users with Read-Write access will be able to modify all modifiable parameters in **set** and **show** commands, as well as view Read-Only commands. Administrators or Super Users will be allowed all Read-Write and Read-Only privileges, and will be able to modify local user accounts. The Matrix Series device indicates which mode a user is logged in as by displaying one of the following prompts:

- Admin: Matrix(su)->
- Read-Write: Matrix(rw)->
- Read-Only: Matrix(ro)->

Downloaded from www.Manualslib.com manuals search engine

Note: Depending on which Matrix Series device you are using, your default command prompt may be different than the examples shown.

Using WebView

By default WebView (Enterasys Networks' embedded web server for device configuration and management tasks) is enabled on TCP port number 80 of the Matrix Series device. You can verify WebView status, enable or disable WebView, as described in the following section.

Displaying WebView status:

To display WebView status, enter **show webview** at the CLI command prompt.

This example shows that WebView is enabled on TCP port 80, the default port number.

```
Matrix(rw)->show webview
 WebView is Enabled. Configured listen port is 80.
```

Enabling / disabling WebView:

To enable or disable WebView, enter **set webview** {**enable** o **disable**} at the CLI command prompt.

This example shows how to enable WebView.

```
Matrix(rw)->set webview enable
```

Starting and Navigating the Command Line Interface

Using a Console Port Connection

Note: By default, the Matrix Series device is configured with three user login accounts: **ro** for Read-Only access; **rw** for Read-Write access; and **admin** for super-user access to all modifiable parameters. The default password is set to a blank string. For information on changing these default settings, refer to "Setting User Accounts and Passwords" on page 2-15.

Once you have connected a terminal to the local console port as described in your *Matrix Series Installation Guide*, the startup screen, Figure 2-1, will display. You can now start the Command Line Interface (CLI) by

- Using a default user account, as described in "Logging in with a Default User Account" on page 2-7, or
- Using an administratively-assigned user account as described in "Logging in with Administratively Configured Account" on page 2-8.

Logging in with a Default User Account

If this is the first time your are logging in to the Matrix Series device, or if the default user accounts have not been administratively changed, proceed as follows:

1. At the login prompt, enter one of the following default user names:
   - **ro** for Read-Only access,
   - **rw** for Read-Write access.
   - **admin** for Super User access.
2. Press ENTER. The Password prompt displays.

Downloaded from www.Manualslib.com manuals search engine

3. Leave this string blank and press ENTER. The device information and Matrix prompt displays as shown in Figure 2-1.

Logging in with Administratively Configured Account

If the device's default user account settings have been changed, proceed as follows:

1. At the login prompt, enter your administratively-assigned user name and press ENTER.
2. At the Password prompt, enter your password and press ENTER.

The notice of authorization and the Matrix prompt displays as shown in Figure 2-1.

Note: Users with Read-Write (rw) and Read-Only access can use the **set password** command ("set password" on page 2-18) to change their own passwords. Administrators with Super User (su) access can use the **set system login** command ("set system login" on page 2-16) to create and change user accounts, and the **set password** command to change any local account password.

Using a Telnet Connection

Once the Matrix Series device has a valid IP address, you can establish a Telnet session from any TCP/IP based node on the network as follows.

1. Telnet to the device's IP address.
2. Enter login (user name) and password information in one of the following ways:
   - If the device's default login and password settings have not been changed, follow the steps listed in "Logging in with a Default User Account" on page 2-7, or
   - Enter an administratively-configured user name and password.

The notice of authorization and the Matrix prompt displays as shown in Figure 2-1.

For information about setting the IP address, refer to "set ip address" on page 2-31.

For information about configuring Telnet settings, refer to "Starting and Configuring Telnet" on page 2-76.

Refer to the instructions included with the Telnet application for information about establishing a Telnet session.

Figure 2-1 Matrix DFE-Gold Startup Screen

```
login: admin
Password:



M A T R I X DFE GOLD

Command Line Interface

Enterasys Networks, Inc.
50 Minuteman Rd.
Andover, MA 01810-1008 U.S.A.

Phone:  +1 978 684 1000
E-mail: support@enterasys.com
WWW:    http://www.enterasys.com
```


Downloaded from www.Manualslib.com manuals search engine

```
(c) Copyright Enterasys Networks, Inc. 2005

ModuleChassis Serial Number: 1234567
ModuleChassis Firmware Revision: 05.11.00

Matrix DFE Gold(su)->
```

Getting Help with CLI Syntax

The Matrix Series device allows you to display usage and syntax information for individual commands by typing **help** or **?** after the command.

Using Context-Sensitive Help

Entering **help** after a specific command will display usage and syntax information for that command. This example shows how to display context-sensitive help for the **set length** command:

```
Matrix(rw)->set length help
Command: set length Number of lines
Usage:  set length  <screenlength>
        screenlength     Length of the screen (5..512, 0 to disable 'more')
```

Performing Keyword Lookups

Entering a space and a question mark (**?**) after a keyword will display all commands beginning with the keyword. Figure 2-2 shows how to perform a keyword lookup for the **show snmp** command. In this case, 13 additional keywords are used by the **show snmp** command. Entering a space and a question mark (**?**) after any of these parameters (such as **show snmp user**) will display additional parameters nested within the syntax.

Figure 2-2 Performing a Keyword Lookup

```
Matrix(rw)->show snmp ?
  access           SNMP VACM access configuration
  community        SNMP v1/v2c community name configuration
  context          SNMP VACM context list
  counters         SNMP counters
  engineid         SNMP engine properties
  group            SNMP VACM security to group configuration
  notify           SNMP notify configuration
  notifyfilter     SNMP notify filter configuration
  notifyprofile    SNMP notify profile configuration
  targetaddr       SNMP target address configuration
  targetparams     SNMP target parameters configuration
  user             SNMP USM user configuration
  view             SNMP VACM view tree configuration
Matrix(rw)->show snmp
Matrix(rw)->show snmp user ?
  list             List usernames
  <user>           User name
```


Downloaded from www.Manualslib.com manuals search engine

```
  remote           Show users with remote SNMP engine ID
  volatile         Show temporary entries
  nonvolatile      Show permanent entries
  read-only        Show r/o entries
  <cr>
Matrix(rw)->show snmp user
```

Entering a question mark (**?**) without a space after a partial keyword will display a list of commands that begin with the partial keyword. Figure 2-3 shows how to use this function for all commands beginning with **co**:

Figure 2-3 Performing a Partial Keyword Lookup

```
Matrix(rw)->co?
  configure        Execute a configuration file
  copy             Upload or download an image or configuration file
Matrix(rw)->co
```



Note: At the end of the lookup display, the system will repeat the command you entered without the ?.

Displaying Scrolling Screens

If the CLI screen length has been set using the **set length** command as described in "set length" on page 2-52, CLI output requiring more than one screen will display --More-- to indicate continuing screens. To display additional screen output:

- Press any key other than ENTER to advance the output one screen at a time.
- Press ENTER to advance the output one line at a time.

The example in Figure 2-4 shows how the **show mac** command indicates that output continues on more than one screen.

Figure 2-4 Scrolling Screen Output

```
Matrix(rw)->show mac


MAC Address           FID       Port      Type
 ------------------------------------------------------------
 00-00-1d-67-68-69      1       host.0.1  learned
 00-00-02-00-00-00      1       fe.1.2    learned
 00-00-02-00-00-01      1       fe.1.3    learned
 00-00-02-00-00-02      1       fe.1.4    learned
 00-00-02-00-00-03      1       fe.1.5    learned
 00-00-02-00-00-04      1       fe.1.6    learned
 00-00-02-00-00-05      1       fe.1.7    learned
 00-00-02-00-00-06      1       fe.1.8    learned
 00-00-02-00-00-07      1       fe.1.9    learned
 00-00-02-00-00-08      1       fe.1.10   learned
--More--
```


Downloaded from www.Manualslib.com manuals search engine

Abbreviating and Completing Commands

The Matrix Series device allows you to abbreviate CLI commands and keywords down to the number of characters that will allow for a unique abbreviation. Figure 2-5 shows how to abbreviate the **show netstat** command to **sh net**.

Figure 2-5 Abbreviating a Command

```
Matrix(rw)->sh net
Active Internet connections (including servers)
Proto Recv-Q Send-Q  Local Address          Foreign Address        State
----- ------ ------  -------------------- --------------------- -------
TCP        0      0  10.21.73.13.23        134.141.190.94.51246  ESTABLISHED
TCP        0    275  10.21.73.13.23        134.141.192.119.4724  ESTABLISHED
TCP        0      0  *.80                  *.*                   LISTEN
TCP        0      0  *.23                  *.*                   LISTEN
UDP        0      0  10.21.73.13.1030      134.141.89.113.514
UDP        0      0  *.161                 *.*
UDP        0      0  *.1025                *.*
UDP        0      0  *.123                 *.*
```

Using the Spacebar Auto Complete Function

When the spacebar auto complete function is enabled, pressing the spacebar after a CLI command fragment will allow you to determine if the fragment is unique. If it is, the CLI will complete the fragment on the current display line.

By default, this function is disabled. For more information on enabling it using the **set cli completion** command, refer to "set cli completion" on page 2-45. Figure 2-6 shows how, when the function is enabled, entering **conf** and pressing the spacebar would be completed as configure:

Figure 2-6 Completing a Partial Command

```
Matrix(rw)->conf<SPACEBAR>
Matrix(rw)->configure
```

Configuring the Line Editor

The command line editor determines which key sequences can be used in the CLI. Example: Ctrl+A will move the cursor to beginning of the command line when in Emacs mode. The CLI supports both vi and Emacs-like line editing commands. By default, the "default" line-editing mode is configured, with no special key sequences. See Table 2-7 lists some commonly used Emacs and vi commands. Use the **set line-editor** command ("set line-editor" on page 2-14) to change the line-editor mode.

Figure 2-7 Basic Line Editing Emacs & vi Commands

Key Sequence	Emacs Command
Ctrl+A	Move cursor to beginning of line.
Ctrl+B	Move cursor back one character.
Ctrl+C	Abort command.
Ctrl+D	Delete a character.

Downloaded from www.Manualslib.com manuals search engine

Figure 2-7 Basic Line Editing Emacs & vi Commands (continued)

Key Sequence	Emacs Command
Ctrl+E	Move cursor to end of line.
Ctrl+F	Move cursor forward one character.
Ctrl+H	Delete character to left of cursor.
Ctrl+I or TAB	Complete word.
Ctrl+K	Delete all characters after cursor.
Ctrl+L or Ctrl+R	Re-display line.
Ctrl+N	Scroll to next command in command history (use the CLI **history** command to display the history).
Ctrl+P	Scroll to previous command in command history.
Ctr1+Q	Resume the CLI process.
Ctr1+S	Pause the CLI process (for scrolling).
Ctrl+T	Transpose characters.
Ctrl+U or Ctrl+X	Delete all characters before cursor.
Ctrl+W	Delete word to the left of cursor.
Ctrl+Y	Restore the most recently deleted item.
h	Move left one character
l	Move right one character
k	Get previous shell command in history
j	Get next shell command in history
$	Go to end of line
0	Go to beginning of line
a	Append
A	Append at end of line
c SPACE	Change character
cl	Change character
cw	Change word
cc	Change entire line
c$	Change everything from cursor to end of line
i	Insert
I	Insert at beginning of line
R	Type over characters
*n*rc	Replace the following *n* characters with *c*
*n*x	Delete *n* characters starting at cursor
*n*X	Delete *n* characters to the left of the cursor
d SPACE	Delete character

Downloaded from www.Manualslib.com manuals search engine

Figure 2-7 Basic Line Editing Emacs & vi Commands (continued)

Key Sequence	Emacs Command
dl	Delete character
dw	Delete word
dd	Delete entire line
d$	Delete everything from cursor to end of line
D	Same as “d$”
p	Put last deletion after the cursor
P	Put last deletion before the cursor
u	Undo last command
~	Toggle case, lower to upper or vice versa

Commands

For information about...	Refer to page...
show line-editor	2-13
set line-editor	2-14

show line-editor

Use this command to show current and default line-editor mode and Delete character mode.

Syntax

show line-editor

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Only.

Example

This example shows how to view the current and default line-editor mode and Delete mode:

```
Matrix(rw)->show line-editor
Current Line-Editor mode is set to: EMACS
Default Line-Editor mode is set to: Default

Current DEL mode is set to: delete
System DEL mode is set to: delete
```


Downloaded from www.Manualslib.com manuals search engine

set line-editor

Use this command to set the current and default line editing mode or the way the Delete character is treated by the line editor. You can also set the persistence of your line editing selections.

Syntax

set line-editor {**emacs** | **vi** | **default** | **delete** {**backspace** | **delete**}} [**default**]

Parameters

emacs	Selects emacs command line editing mode. See Table 2-7 for some commonly used emacs commands.
vi	Selects vi command line editing mode.
default	Selects default line editing mode.
delete {**backspace** | **delete**}	Sets the way the line editor treats the Delete ASCII character. **delete backspace** — the line editor will treat Delete (0x7f) as a Backspace (0x08) character. **delete delete** — the line editor will treat Delete as the Delete character (the default condition).
default	(Optional) Make the line editor or Delete mode setting persist for all future sessions.

Defaults

If **default** is not entered after selecting a line editing or Delete mode, the selection will apply only to the current session and will not persist for future sessions.

Mode

Switch command, Read-Write.

Examples

This example sets the current line-editor to vi mode:

```
Matrix(rw)->set line-editor vi
```

This example sets the default line-editor to emacs mode and sets the selection to persist for future sessions:

```
Matrix(rw)->set line-editor emacs default
```


Downloaded from www.Manualslib.com manuals search engine

Setting User Accounts and Passwords

Purpose

To change the device's default user login and password settings, and to add new user accounts and passwords.

Commands

For information about...	Refer to page...
show system login	2-15
set system login	2-16
clear system login	2-17
set password	2-18
show system password	2-19
set system password	2-20
clear system password	2-22
show system lockout	2-23
set system lockout	2-24

show system login

Use this command to display user login account information.

Syntax

show system login

Parameters

None.

Defaults

None.

Mode

Switch command, Super User.

Example

This example shows how to display login account information. In this case, device defaults are user names **admin**, **ro,** and **rw** and have not been changed. **bar** and **foo** are user configured accounts:

```
Matrix(su)->show system login
Username        Access      State     Local  Login Access Allowed
                                      Only?  Start  End   Days
```


Downloaded from www.Manualslib.com manuals search engine

```
admin           super-user  enabled   no     ***access always allowed***
bar             read-only   enabled   yes    00:00 24:00  Sun Sat
foo             read-write  enabled   no     08:00 17:00  Mon Tue Wed Thu Fri
ro              read-only   enabled   no     ***access always allowed***
rw              read-write  enabled   no     ***access always allowed***
```

Table 2-3 provides an explanation of the command output.

Table 2-3 show system login Output Details

Output...	What it displays...
Password history size	Number of previously used user login passwords that will be checked for duplication when the **set password** command is executed. Configured with **set system password history** ("set system password" on page 2-20).
Password aging	Number of days user passwords will remain valid before aging out. Configured with **set system password aging** ("set system password" on page 2-20).
Username	Login user names.
Access	Access assigned to this user account: **super-user**, **read-write** or **read-only**.
State	Whether this user account is **enabled** or **disabled**.
Local Only?	Specifies authentication scope for this user. Valid values: yes, no. yes specifies that authentication is only by way of the local user database even with RADIUS or TACACS+ configured. no specifies that authentication is via configured methods.
Login Access Allowed	Specifies the time periods by start and end in 24 hour time and the days of the week for which access is allowed, or states that access is always allowed.

set system login

Use this command to create a new user login account, or to disable or enable an existing account. The Matrix Series device supports up to 16 user accounts, including the admin account, which cannot be disabled or deleted.

Syntax

set system login *username* {**super-user** | **read-write** | **read-only**} {**enable** | **disable**} [**password** *password*] [**allowed-interval** *HH:MM HH:MM*] [**allowed-days** {[**Sun**] [**Mon**] [**Tue**] [**Wed**] [**Thu**] [**Fri**] [**Sat**]}] [**local-only** {**yes** | **no**}]

Parameters

username	Specifies a login name for a new or existing user. This string can be a maximum of 80 characters, although a maximum of 16 characters is recommended for proper viewing in the **show system login** display.
super-user | **read-write** | **read-only**	Specifies the access privileges for this user.
enable | **disable**	Enables or disables the user account. **Note:** The default admin (**su**) account cannot be disabled.

Downloaded from www.Manualslib.com manuals search engine

password *password*	(Optional) Specifies the encrypted password for this user account. **NOTE:** This option is intended only for use in configurations generated by the **show config** command.
allowed-interval *HH:MM HH:MM*	(Optional) Specifies the start and end hour *HH* and minute *MM* time period for which access will be allowed for this user based upon 24 hour time.
allowed-days	(Optional) Specifies at least 1 and up to 7 days of the week for which access will be allowed for this user.
local-only	(Optional) Specifies the authentication scope for this user. Valid values: **yes**, **no**. **yes** specifies that authentication is only by way of the local user database even with RADIUS or TACACS+ configured. **no** specifies that authentication is by way of configured methods.

Defaults

allowed-interval: 00:00-24:00 (all hours allowed)

allowed-days: Sun, Mon, Tue, Wed, Thu, Fri, Sat (all days allowed)

local-only: no.

Mode

Switch command, Super User.

Allowed interval and allowed days may be configured on any user account but are not enforced on super-user accounts.

Example

This example shows how to enable a new user account with the login name **netops** with super user access privileges:

```
Matrix(su)->set system login netops super-user enable
```

clear system login

Use this command to remove a local login user account or to reset a specified option to its default value.

Syntax

clear system login *username* [**allowed-interval**] [**allowed-days**] [**local-only**]

Parameters

username	Specifies the login name of the account to be cleared if no optional parameters are specified. If an optional parameter(s) is specified, the account is not cleared and the specified parameter(s) is reset to the default value. **Note:** The default admin (su) account cannot be deleted.
allowed-interval	(Optional) When specified, the configured allowed interval setting is reset to the default value.

Downloaded from www.Manualslib.com manuals search engine

allowed-days	(Optional) When specified, the configured allowed days setting is reset to the default value.
local-only	(Optional) When specified, the configured local only setting is reset to the default value.

Defaults

The account is removed if no optional parameters are entered.

Mode

Switch command, Super User.

Example

This example shows how to remove the "netops" user account:

```
Matrix(su)->clear system login netops
```

set password

Use this command to change system default passwords or to set a new login password on the CLI.

Syntax

set password [*username*]

Parameters

username	(Only available to users with super-user access.) Specifies a system default or a user-configured login account name. By default, the Matrix Series device provides the following account names: • **ro** for Read-Only access, • **rw** for Read-Write access. • **admin** for Super User access. (This access level allows Read-Write access to all modifiable parameters, including user accounts.)

Defaults

None.

Mode

Switch command. Read-Write users can change their own passwords. Super Users (Admin) can change any password on the system.

Usage

Only users with admin (**su**) access privileges can change any password on the system.

Users with Read-Write (**rw**) access privileges can change their own passwords, but cannot enter or modify other system passwords.

Passwords must be a minimum of 8 characters and a maximum of 40 characters.

If configured, password length must conform to the minimum number of characters set with the **set system password length** command ("set system password" on page 2-20).

Downloaded from www.Manualslib.com manuals search engine

The **admin** password can be reset by toggling dip switch 8 on the device as described in your *Matrix Series Installation Guide*.

Examples

This example shows how a super-user would change the Read-Write password from the system default (blank string):

```
Matrix(su)->set password rw
Please enter new password: ********
Please re-enter new password: ********
Password changed.
Matrix(su)->
```

This example shows how a user with Read-Write access would change his password:

```
Matrix(rw)->set password
Please enter old password: ********
Please enter new password: ********
Please re-enter new password: ********
Password changed.
Matrix(rw)->
```

show system password

Use this command to display current password configuration settings.

Syntax

show system password

Parameters

None.

Defaults

None.

Mode

Switch command, Super User.

Example

This example shows how to display password configuration settings. In this case, the settings displayed are the default settings:

```
Matrix(su)->show system password
Password history size  : 0
Password aging         : disabled
Password minimum length: 8
Password minimum character requirements:
   Uppercase: 0
   Lowercase: 0
```


Downloaded from www.Manualslib.com manuals search engine

```
     Numeric: 0
     Special: 0
Password assignment required at account creation                        : no
Allow multiple accounts to share same password                          : yes
Length of substrings in previous password(s) not allowed in new password: 0
Allow the same character to appear consecutively in a password          : yes
Require non-superusers to change password at first login                : no
Minimum interval between password changes by non-superusers           : 0 minutes
```

set system password

Use this command to configure system password parameters.

Syntax

set system password [**aging** {*days* | **disable**}]
[**history** {*size*}]
[**length** {*#ofChars*}]
[**min-required-chars** {[**uppercase** *#ofChars*] [**lowercase** *#ofChars*] [**numeric** *#ofChars*] [**special** *#ofChars*]}]
[**require-at-creation** {**yes** | **no**}]
[**allow-duplicates** {**yes** | **no**}]
[**substring-match-len** *#ofChars*]
[**allow-repeating-chars** {**yes** | **no**}]
[**change-first-login** {**yes** | **no**}]
[**change-frequency** *minutes*]

Parameters

aging *days* | **disable**	Specifies the number of days to age the password. • *days* - Valid values are **1** - **365** • **disable** - Aging is not taken into account for user account passwords.
history *size*	Specifies the number of passwords to keep in the password history for a user account. Valid values: **0** - **10**.
length *#ofChars*	Specifies the minimum number of characters in a user account password.
min-required-chars	Specifies the minimum number of characters of the specified type that must be present in a user account password as follows: • **uppercase** *#ofchars* - minimum number of upper case characters • **lowercase** *#ofchars* - minimum number of lower case characters • **numeric** *#ofchars* - minimum number of numeric characters • **special** *#ofchars* - minimum number of special characters Valid values: **0** - **40** in all cases.

Downloaded from www.Manualslib.com manuals search engine

require-at-creation	Specifies whether a password is required at the time of user account creation: • **yes** - Password is required when creating a user account • **no** - Password is not required when creating a user account
allow-duplicates	Specifies whether multiple accounts can share the same password: • **yes** - Specifies that multiple accounts may share the same password • **no** - Specifies that multiple accounts may not share the same password
substring-match-len *#ofChars*	Specifies the length of any substring present in a previous password(s) for this account that may not be used in a new password. Valid values: **0** - **40**.
allow-repeating-chars	Specifies whether the same character may appear consecutively in the same password: • **yes** - specifies that the same character may appear consecutively in a password • **no** - specifies that the same character may not appear consecutively in a password
change-first-login	Specifies whether new users are required to change their password upon first login: • **yes** - specifies that new users must change the password for this account upon first login • **no** - specifies that new users are not required to change the password for this account upon first login
change-frequency *minutes*	Specifies a minimum interval in minutes between password changes allowed for non-superusers. Valid values: **0** - **65535**.

Defaults

aging = **disable**

history = **0** passwords

length = **8** characters

min-required-chars = 0 characters for all cases

require-at-creation = **No**. Password is not required at user account creation.

allow-duplicates = **Yes**. Multiple accounts may use the same password.

substring-match-len = **0** characters.

allow-repeating-chars = **Yes**. Consecutive use of the same character in a password is allowed.

change-first-login = **No**. The password does not have to be changed upon first login.

change-frequency = **0** minutes.

Mode

Switch command. Super User.

Usage

The set of special characters recognized by this command is: !@#$%^&*()-=[]\;?,./`.

Downloaded from www.Manualslib.com manuals search engine

If the **require-at-creation** option is enabled, the **set system login** command will interactively prompt for a cleartext password upon creation of a new user account. It will be as if a **set password** *username* command was implicitly executed. The new account will not be successfully created until a valid password has been specified. A cleartext password will not be solicited if an encrypted password is already specified by way of the **set system login** command's **password** option.

If the **allow-duplicates** option is set to **no**, a user will not be able to select as a new password one which is already being used by another user.

If a **substring-match-len** option is set to zero, no substring matching will be performed when validating new passwords. If the **substring-match-len** option is configured with a nonzero length, any substring of the specified length appearing in the current password for this user may not appear in a new password. If the configured **history** size is nonzero, then all historical passwords up to that size will also be compared with the input of the new password. Any substring of the configured length appearing in any of the historical passwords may not be used in the new password. This option is not enforced when a password is changed by a superuser.

A password **change-frequency** interval of zero means there is no restriction on the frequency of password changes.

A configured minimum **change-frequency** interval applies only to users without super-user privileges attempting to change their own passwords. Users with super-user privileges may change their passwords at any time.

Example

This example shows how to set the age of a system password for 60 days, the minimum lenght of the password to 6 and that the same character can not repeat consecutively in the same password:

```
Matrix(su)->set system password age 60 length 6 allow-repeating-chars no
```

clear system password

Use this command to set local login password parameters to default values.

Syntax

set system password [**aging**] [**history** *size*] [**length** *#ofChars*] [**min-required-chars** {[**uppercase**] [**lowercase**] [**numeric**] [**special**]}] [**require-at-creation**] [**allow-duplicate**] [**substring-match-len** *#ofChars*] [**allow-repeating-chars**] [**change-first-login**] [**change-frequency** *minutes*]

Parameters

aging	Specifies that the number of days to age the password be reset to the default value.
history *size*	Specifies that the number of passwords to keep in the password history for a user account be reset to the default value.
length *#ofChars*	Specifies that the minimum number of characters that must be present in a user account password be reset to the default value.
min-required-chars	Specifies that the minimum number of characters of the specified type that must be present in a user account password be set to the default value: **uppercase, lowercase, numeric, special**
require-at-creation	Specifies that the requirement that a password be configured at the time of user account creation be set to the default value.

Downloaded from www.Manualslib.com manuals search engine

allow-duplicates	Specifies that the option controlling whether multiple accounts can share the same password be set to the default value.
substring-match-len *#ofChars*	Specifies that the length of any substring present in a previous password(s) for this account that may not be used in a new password be set to the default value.
allow-repeating-chars	Specifies that the option controlling whether the same character may appear consecutively in the same password be set to the default value.
change-first-login	Specifies that the option controlling whether new users are required to change their password upon first login be set to the default value.
change-frequency *minutes*	Specifies that the minimum interval between password changes be set to the default value.

Defaults

If no options are specified, options are reset to default values.

Mode

Switch comman, Super User.

Example

This example shows how to reset the minimum system password length to the default number of characters:

```
Matrix(su)->clear system password length
```

show system lockout

Use this command to display settings for locking out users.

Syntax

show system lockout

Parameters

None.

Defaults

None.

Mode

Switch command, Super User.

Example

This example shows how to display user lockout settings. In this case, device defaults have not been changed:

```
Matrix(su)->show system lockout
Unsuccessful login attempts before account lockout       : 3
Duration of lockout (superuser accounts only)            : 15 minutes
Period of inactivity before non-superuser account lockout: 0 days
```


Downloaded from www.Manualslib.com manuals search engine

Table 2-4 provides an explanation of the command output. These settings are configured with the **set system lockout** command ("set system lockout" on page 2-24).

Table 2-4 show system lockout Output Details

Output...	What it displays...
Unsuccessful login attempts	Number of failed login attempts allowed before a read-write or read-only user's account will be disabled.
Duration of lockout	Number of minutes the default admin user account will be locked out after the maximum login attempts.
Period of inactivity	Number of days of inactivity before a non-superuser account is locked out. Zero specifies no lockout will occur for inactivity.

set system lockout

Use this command to set the number of failed login attempts before locking out (disabling) a read-write or read-only user account, the number of minutes to lockout the default admin super user account after maximum login attempts, and the number of inactive days before a non-superuser account is locked out.

Syntax

set system lockout {[**attempts** *attempts*] [**time** *minutes*] [**inactive** *days*]}

Parameters

attempts *attempts*	Specifies the number of failed login attempts allowed before a read-write or read-only user's account will be disabled. Valid values are **1** to **15**.
time *minutes*	Specifies the number of minutes the default admin user account will be locked out after the maximum login attempts. Valid values are **0** to **65565**.
inactive *days*	Specifies the period of inactivity in days after which a non-superuser account will be locked out. Valid values are **0** to **65565**.

Defaults

attempts: 3

time: 15 minutes

inactive: 0 days.

Mode

Switch command, Super User.

Usage

An inactivity timer value of zero means that no account will be locked out due to inactivity.

Once a user account is locked out, it can only be re-enabled by a super user with the **set system login** command ("set system login" on page 2-16).

Downloaded from www.Manualslib.com manuals search engine

Example

This example shows how to set login attempts to 5 and lockout time to 30 minutes and the inactivity timer to 60 days:

```
Matrix(su)->set system lockout attempts 5 time 30 inactive 60
```


Downloaded from www.Manualslib.com manuals search engine

Managing the Management Authentication Notification MIB

Purpose

This MIB provides controls for enabling/disabling the sending of SNMP notifications when a user login authentication event occurs for various management access types. The types of access currently supported by the MIB include console, telnet, ssh, and web.

Commands

The CLI commands used to set the Management Authentication Notification are listed below and described in the associated section as shown.

For information about...	Refer to page...
show mgmt-auth-notify	2-26
set mgmt-auth-notify	2-27
clear mgmt-auth-notify	2-28



Note: Ensure that SNMP is correctly configured on the DFE in order to send these notifications. Refer to Chapter 5 for SNMP configuration information.

show mgmt-auth-notify

Use this command to display the current setting for the Management Authentication Notification MIB.

Syntax

show mgmt-auth-notify

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Only.

Example

This example shows how to display the current information for the Management Authentication Notification.:

```
Matrix(su)->show mgmt-auth-notify

Management Type  Status
---------------  --------
console          enabled
```


Downloaded from www.Manualslib.com manuals search engine

```
ssh             enabled
telnet          enabled
web             enabled
```

set mgmt-auth-notify

Use this command to either enable or disable the Management Authentication Notification MIB. By selecting the optional Management access type, a user can specifically enable or disable a single access type, multiple access types or all of the access types. The default setting is that all Management Authentication Notification types are enabled.

Syntax

set mgmt-auth-notify {**enable** | **disable**}{**console** | **ssh** | **telnet** | **web**}

Parameters

enable	Enables selected or all notifications.
disable	Disables selected or all notifications.
console	(Optional) sets the console authentications
ssh	(Optional) sets SSH authentications
telnet	(Optional) sets telnet authentications
web	(Optional) sets web authentications

Defaults

If none of the optional Management Authentication Access types are entered, than all authentications types listed above will either be enabled or disabled.

Mode

Switch command, Read-Write.

Usage

Insure that SNMP is correctly configured on the DFE in order to send these notifications, refer to the following chapter for configuring SNMP (Chapter 5).

Examples

This example shows how to set all the authentication types to be disabled on the Management Authentication Notification MIB. That information is then displayed with the **show** command:

```
Matrix(su)->set mgmt-auth-notify disable
Matrix(su)->show mgmt-auth-notify

Management Type  Status
---------------  --------
console          disabled
ssh              disabled
telnet           disabled
web              disabled
```


Downloaded from www.Manualslib.com manuals search engine

This example shows how to set only the console and telnet authentication access types to be enabled on the Management Authentication Notification MIB. That information is then displayed with the **show** command.:

```
Matrix(su)->set mgmt-auth-notify enable console telnet
Matrix(su)->show mgmt-auth-notify

Management Type  Status
---------------  --------
console          enabled
ssh              disabled
telnet           enabled
web              disabled
```

clear mgmt-auth-notify

Use this command to set the current setting for the Management Authentication Notification access types to the default setting of enabled.

Syntax

clear mgmt-auth-notify

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Write.

Usage

Ensure that SNMP is correctly configured on the DFE in order to send these notifications. Refer to Chapter 5 for SNMP configuration information.

Example

This example displays the state of Management Authentication Notification access types prior to using the **clear** command, then displays the same information after using the **clear** command:

```
Matrix(su)->show mgmt-auth-notify

Management Type  Status
---------------  --------
console          enabled
ssh              disabled
telnet           enabled
web              disabled
```


Downloaded from www.Manualslib.com manuals search engine

```
Matrix(su)->clear mgmt-auth-notify

Matrix(su)->show mgmt-auth-notify

Management Type  Status
---------------  --------
console          enabled
ssh              enabled
telnet           enabled
web              enabled
```


Downloaded from www.Manualslib.com manuals search engine

Setting Basic Device Properties

Purpose

To display and set the system IP address and other basic system (device) properties, including time, contact name and alias, physical asset IDs for modules, terminal output, timeout, and version information.

Commands

For information about...	Refer to page...
show ip address	2-31
set ip address	2-31
clear ip address	2-32
show ip gratuitous-arp	2-32
set ip gratuitous-arp	2-33
clear ip gratuitous-arp	2-33
show system	2-34
show system hardware	2-35
show system utilization	2-37
set system utilization threshold	2-39
clear system utilization	2-40
show time	2-40
set time	2-41
show summertime	2-41
set summertime	2-42
set summertime date	2-42
set summertime recurring	2-43
clear summertime	2-44
set prompt	2-44
set cli completion	2-45
loop	2-45
show banner	2-46
set banner	2-47
clear banner	2-48
show version	2-48
set system name	2-50
set system location	2-50

Downloaded from www.Manualslib.com manuals search engine

For information about...	Refer to page...
set system contact	2-51
set width	2-51
set length	2-52
show logout	2-52
set logout	2-53
show physical alias	2-53
set physical alias	2-54
clear physical alias	2-55
show physical assetid	2-55
set physical assetid	2-56
clear physical assetid	2-56

show ip address

Use this command to display the system IP address and subnet mask.

Syntax

show ip address

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Only.

Example

This example shows how to display the system IP address and subnet mask:

```
Matrix(rw)->show ip address
Name                    Address                 Mask
----------------        ----------------        ----------------
host                    10.42.13.20             255.255.0.0
```

set ip address

Use this command to set the system IP address, subnet mask and default gateway.

Syntax

set ip address *ip-address* [**mask** *ip-mask*] [**gateway** *ip-gateway*]

Downloaded from www.Manualslib.com manuals search engine

Parameters

ip-address	Sets the IP address for the system.
mask *ip-mask*	(Optional) Sets the system's subnet mask.
gateway *ip-gateway*	(Optional) Sets the system's default gateway (next-hop device).

Defaults

If not specified, *ip-mask* will be set to the natural mask of the *ip-address* and *ip-gateway* will be set to the *ip-address*.

Mode

Switch command, Read-Write.

Example

This example shows how to set the system IP address to 10.1.10.1 with a mask of 255.255.128.0 and a default gateway of 10.1.0.1:

```
Matrix(rw)->set ip address 10.1.10.1 mask 255.255.128.0 gateway 10.1.10.1
```

clear ip address

Use this command to clear the system IP address.

Syntax

clear ip address

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to clear the system IP address:

```
Matrix(rw)->clear ip address
```

show ip gratuitous-arp

Use this command to display the gratuitous ARP processing behavior.

Syntax

show ip gratuitous-arp

Downloaded from www.Manualslib.com manuals search engine

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Only.

Example

This example shows how to display the IP gratuitous-arp process for both requests and replies.

Matrix(rw)->show ip gratuitous-arp

```
Processing gratuitous ARP requests and replies.
```

set ip gratuitous-arp

Use this command to control the gratuitous ARP processing behavior.

Syntax

set ip gratuitous-arp [**request**] [**reply**] [**both**]]

Parameters

request	Process only gratuitous ARP requests.
reply	Process only gratuitous ARP replies.
both	Process both requests and replies.

Defaults

Disabled by default

Mode

Switch command, Read-Write.

Example

This example sets both gratuitous ARP requests and replies:

```
Matrix(rw)->set ip gratuitous-arp both
```

clear ip gratuitous-arp

Use this command to stop all gratuitous ARP processing.

Syntax

clear ip gratuitous-arp

Downloaded from www.Manualslib.com manuals search engine

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to clear the gratuitous-arp processing:

```
Matrix(rw)->clear ip gratuitous-arp
```

show system

Use this command to display system information, including contact information, power and fan tray status and uptime.

Syntax

show system

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Only.

Example

This example shows how to display system information:

```
Matrix(rw)->show system
System contact:
System location:
System name:

PS1-Status     PS2-Status
-------------  -------------
ok             not installed

Fan1-Status
-------------
ok
```


Downloaded from www.Manualslib.com manuals search engine

```
Temp-Alarm     Uptime d,h:m:s  Logout
-------------  --------------  -------------
off                0,19:40:00  10 min

PS1-Type       PS2-Type
-------------  -------------
6C207-1        not installed
```

Table 2-5 provides an explanation of the command output.

Table 2-5 Show System Output Display

Output...	What it displays...
System contact	Contact person for the system. Default of a blank string can be changed with the **set system contact** command (“set system contact” on page 2-51).
System location	Where the system is located. Default of a blank string can be changed with the **set system location** command (“set system location” on page 2-50).
System name	Name identifying the system. Default of a blank string can be changed with the **set system name** command (“set system name” on page 2-50).
PS1 and PS2-Status	Operational status for power supply 1 and, if installed, power supply 2.
Fan Status	Operational status of the fan tray.
Temp-Alarm	Whether or not the system temperature alarm is off (within normal temperature range) or on.
Uptime d,h:m:s	System uptime.
Logout	Time an idle console or Telnet CLI session will remain connected before timing out. Default of 15 minutes can be changed with the **set logout** command (“set logout” on page 2-53).
PS1 and PS2-Type	Model number of power supply 1 and, if installed, power supply 2.

show system hardware

Use this command to display the system’s hardware configuration.

Syntax

show system hardware

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Only.

Downloaded from www.Manualslib.com manuals search engine

Example

The following example shows a portion of the information displayed with the **show system hardware** command.



Note: Depending on the hardware configuration of your Matrix system, your output will vary from the example shown.

```
Matrix(rw)->show system hardware

CHASSIS HARDWARE INFORMATION
----------------------------
Chassis Type:                  Matrix N7 Platform
   Chassis Serial Number:      0001a300611b
   Power Supply 1:             Not Installed
   Power Supply 2:             Installed & Operating, AC, Not Redundant
   Chassis Fan:                Installed & Operating

SLOT HARDWARE INFORMATION
-------------------------
SLOT 1
      Model:                   7H4382-494H4282-492G4072-52
      Serial Number:           0123456789AB
      Part Number:             6543210
      Vendor ID:               1
      Base MAC Address:        11-22-33-44-55-66
      Router MAC Address:      11-22-33-44-55-67
      Hardware Version:        5
      Firmware Version:        02.00.13
      BootCode Version:        01.00.07
      CPU Version:             8 (PPC 740/750)
      UpLink:                  Not Present
      SDRAM:                   128 MB
      NVRAM:                   8 KB
      Flash System:            32 MB
         /flash0 free space:   11 MB
         /flash1 free space:   14 MB
Dip Switch Bank  1   2   3   4   5   6   7   8
      Position: OFF OFF OFF OFF OFF OFF OFF OFF
      HOST CHIP
         Revision:             1.0
      FABRIC CHIP              0          1
         Revision:             1.0        1.0
      SWITCH CHIP              0          1          2
         Block ID:             0          1          3
         Revision:             1.50/150   1.50/150   1.50/150
```


Downloaded from www.Manualslib.com manuals search engine

```
   Lookup DDR:          8 MB       8 MB       8 MB
   Transmit DDR:        8 MB       8 MB       8 MB
   Receive DDR:         8 MB       8 MB       8 MB
   Routing DDR:         8 MB       8 MB       8 MB
MAC CHIP                0          1          2
   Model:               FastEnet   FastEnet   FTM1
   Revision:            1          1          0
PHY CHIP 0
   Model:               BCM5226
   Revision:            2
```

show system utilization

Use this command to display system resource utilization information.

Syntax

show system utilization [**cpu** | **process** | **storage**] [**slot** *slot*]

Parameters

cpu | **process** | **storage**	(Optional) Displays total CPU, individual process, or storage resource utilization only.
slot *slot*	(Optional) Displays system resource utilization for a specific module.

Defaults

- If not specified, CPU, process, and storage system utilization information will be displayed.
- If not specified, information for all modules will be displayed.

Mode

Switch command, Read-Only.

Example

This example shows how to display all system utilization information for the module in slot 1:

```
Matrix(rw)->show system utilization slot 1

CPU Utilization Threshold Traps enabled: Threshold = 80.0%

Total CPU Utilization:

Slot    CPU               5 sec   1 min   5 min
-----------------------------------------------------
1      1                  3.6%    3.0%    3.0%

Process Utilization:

Slot: 1 CPU: 1
```


Downloaded from www.Manualslib.com manuals search engine

```
Name                            ProcID 5 sec   1 min   5 min
-------------------------------------------------------------
 CLI                             1        0.0%    0.0%    0.0%
 Chassis Data Synchronization    2        0.0%    0.0%    0.0%
 Connection Maintenance          3        1.0%    0.5%    0.5%
 Hardware Maintenece             4        0.0%    0.0%    0.0%
 Image & Config Management       5        0.0%    0.0%    0.0%
 Persistent Data Management      6        0.0%    0.0%    0.0%
 Runtime Diagnostics             7        0.0%    0.0%    0.0%
 SNMP                            8        0.0%    0.0%    0.0%
 Syslog                          9        0.0%    0.0%    0.0%
 Switch                          10       0.0%    0.0%    0.0%
 Switch CDP                      11       0.0%    0.0%    0.0%
 Switch Dot1x                    12       0.0%    0.0%    0.0%
 Switch Filter Database          13       0.0%    0.0%    0.0%
 Switch GVRP                     14       0.0%    0.0%    0.0%
 Switch Host IP                  15       0.1%    0.1%    0.1%
 Switch IGMP                     16       0.0%    0.0%    0.0%
 Switch LACP                     17       0.0%    0.0%    0.0%
 Switch MAC Authentication       18       0.0%    0.0%    0.0%
 Switch MAC Locking              19       0.0%    0.0%    0.0%
 Switch MTU Discovery            20       0.0%    0.0%    0.0%
 Switch Node & Alias             21       0.0%    0.0%    0.0%
 Switch Packet Processing        22       0.1%    0.1%    0.1%
 Switch POE                      23       0.0%    0.0%    0.0%
 Switch Port Management          24       0.0%    0.0%    0.0%
 Switch PWA                      25       0.0%    0.0%    0.0%
 Switch Radius                   26       0.0%    0.0%    0.0%
 Switch Radius Accounting        27       0.0%    0.0%    0.0%
 Switch RMON                     28       0.0%    0.0%    0.0%
 Switch RMON Capture             29       0.0%    0.0%    0.0%
 Switch SMON                     30       0.0%    0.0%    0.0%
 Switch SNTP                     31       0.0%    0.0%    0.0%
 Switch STP                      32       0.0%    0.0%    0.0%
 Switch UPN                      33       0.0%    0.0%    0.0%

 Name                            ProcID 5 sec   1 min   5 min
-------------------------------------------------------------
 Switch Web Server               34       1.4%    1.4%    1.4%
 Router Misc.                    35       0.0%    0.0%    0.0%
 Router Multicast                36       0.0%    0.0%    0.0%
 Router Control Plane            37       0.0%    0.0%    0.0%
 Router IP                       38       0.0%    0.0%    0.0%
 Router DHCPS                    39       0.0%    0.0%    0.0%
```


Downloaded from www.Manualslib.com manuals search engine

```
 Router OSPF                    40       0.0%    0.0%    0.0%
 Router RIP                     41       0.0%    0.0%    0.0%
 Router VRRP                    42       0.0%    0.0%    0.0%
 Router DVMRP                   43       0.0%    0.0%    0.0%
 Router PIM                     44       0.0%    0.0%    0.0%
 Router PIMDM                   45       0.0%    0.0%    0.0%
 Router ARP                     46       0.0%    0.0%    0.0%
 Router LSNAT                   47       0.0%    0.0%    0.0%
 Interrupts                     48       0.0%    0.0%    0.0%
 OTHER                          49       0.0%    0.0%    0.0%
 IDLE                           50      96.4%   97.0%   97.0%

Storage Utilization:

Slot: 1

Type        Description               Size (Kb)      Available (Kb)
-------------------------------------------------------------------
 RAM        RAM device 1                131072               22192
 Flash      Images & Miscellaneous       16384                4138
 Flash      Nonvolatile Data Storage     16384               14308
```

set system utilization threshold

Use this command to set the threshold for sending CPU utilization notification messages.

Syntax

set system utilization threshold *threshold*

Parameters

threshold	Specifies a threshold value (in 1/10 of a percent).Valid range is **1** - **1000**. A value of **0** will disable utilization notification messages.

Defaults

None.

Mode

Switch command, Read-Write.

Usage

The value range is [1..1000] and represents the % of system utilization to use as the trap threshold.

Example

This example shows how to set the system utilization threshold to 100%:

```
Matrix(rw)->set system utilization threshold 1000
```


Downloaded from www.Manualslib.com manuals search engine

clear system utilization

Use this command to clear the threshold for sending CPU utilization notification messages.

Syntax

clear system utilization

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to clear the system utilization threshold:

```
Matrix(rw)->clear system utilization 1000
```

show time

Use this command to display the current time of day in the system clock.

Syntax

show time

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Only.

Example

This example shows how to display the current time. The output shows the day of the week, month, day, and the time of day in hours, minutes, and seconds and the year:

```
Matrix(rw)->show time
THU SEP 05 09:21:57 2002
```


Downloaded from www.Manualslib.com manuals search engine

set time

Use this command to change the time of day on the system clock.

Syntax

set time [*mm/dd/yyyy*] [*hh:mm:ss*]

Parameters

[*mm/dd/yyyy*] [*hh:mm:ss*]	Sets the time in: • month, day, year and/or • 24-hour format At least one set of time parameters must be entered.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to set the system clock to 7:50 a.m:

```
Matrix(rw)->set time 7:50:00
```

show summertime

Use this command to display daylight savings time settings.

Syntax

show summertime

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Only.

Example

This example shows how to display daylight savings time settings:

```
Matrix(rw)->show summertime

Summertime is disabled and set to ''
Start : SUN MAR 11 02:00:00 2007
```


Downloaded from www.Manualslib.com manuals search engine

```
End   : SUN NOV 04 02:00:00 2007
Offset: 60 minutes (1 hours 0 minutes)
Recurring: yes, starting at 2:00 of the second Sunday of March and ending at 2:00
of the first Sunday of November
```

set summertime

Use this command to enable or disable the daylight savings time function.

Syntax

set summertime {**enable** | **disable**} [*zone*]

Parameters

enable | **disable**	Enables or disables the daylight savings time function.
zone	(Optional) Applies a name to the daylight savings time settings.

Defaults

If a *zone* name is not specified, none will be applied.

Mode

Switch command, Read-Write.

Example

This example shows how to enable daylight savings time function:

```
Matrix(rw)->set summertime enable
```

set summertime date

Use this command to configure specific dates to start and stop daylight savings time.

Syntax

set summertime date *start_month start_date start_year start_hr_min end_month end_date end_year end_hr_min* [*offset_minutes*]

Parameters

start_month	Specifies the month of the year to start daylight savings time.
start_date	Specifies the day of the month to start daylight savings time.
start_year	Specifies the year to start daylight savings time.
start_hr_min	Specifies the time of day to start daylight savings time. Format is hh:mm.
end_month	Specifies the month of the year to end daylight savings time.
end_date	Specifies the day of the month to end daylight savings time.
end_year	Specifies the year to end daylight savings time.

Downloaded from www.Manualslib.com manuals search engine

end_hr_min	Specifies the time of day to end daylight savings time. Format is hh:mm.
offset_minutes	(Optional) Specifies the amount of time in minutes to offset daylight savings time from the non-daylight savings time system setting. Valid values are **1** - **1440**.

Defaults

If an *offset* is not specified, none will be applied.

Mode

Switch command, Read-Write.

Usage

These settings will be non-recurring and will have to be reset annually.

Example

This example shows how to set a daylight savings time start date of April 4, 2004 at 2 a.m. and an ending date of October 31, 2004 at 2 a.m. with an offset time of one hour:

```
Matrix(rw)->set summertime date April 4 2004 02:00 October 31 2004 02:00 60
```

set summertime recurring

Use this command to configure recurring daylight savings time settings.

Syntax

set summertime recurring *start_week start_day start_month start_hr_min end_week end_day end_month end_hr_min* [*offset_minutes*]

Parameters

start_week	Specifies the week of the month to restart daylight savings time. Valid values are: **first**, **second**, **third**, **fourth**, and **last**.
start_day	Specifies the day of the week to restart daylight savings time.
start_hr_min	Specifies the time of day to restart daylight savings time. Format is hh:mm.
end_week	Specifies the week of the month to end daylight savings time.
end_day	Specifies the day of the week to end daylight savings time.
end_hr_min	Specifies the time of day to end daylight savings time. Format is hh:mm.
offset_minutes	(Optional) Specifies the amount of time in minutes to offset daylight savings time from the non-daylight savings time system setting. Valid values are **1** - **1440**.

Defaults

If an *offset* is not specified, none will be applied.

Downloaded from www.Manualslib.com manuals search engine

Mode

Switch command, Read-Write.

Usage

These settings will start and stop daylight savings time at the specified day of the month and hour each year and will not have to be reset annually.

Example

This example shows how set daylight savings time to recur start date of April 4, 2004 at 2 a.m. and an ending date of October 31, 2004 at 2 a.m. with an offset time of one hour:

```
Matrix(rw)->set summertime recurring first Sunday April 02:00 last Sunday October
02:00 60
```

clear summertime

Use this command to clear the daylight savings time configuration.

Syntax

clear summertime

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to clear the daylight savings time configuration:

```
Matrix(rw)->clear summertime
```

set prompt

Use this command to modify the command prompt.

Syntax

set prompt *"prompt_string"*

Parameters

prompt_string	Specifies a text string for the command prompt. **Note:** A prompt string containing a space in the text must be enclosed in quotes as shown in the example below.

Downloaded from www.Manualslib.com manuals search engine

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to set the command prompt to Switch 1:

```
Matrix(rw)->set prompt "Switch 1"
Switch 1(rw)->
```

set cli completion

Use this command to enable or disable the CLI command completion function. When enabled, this allows you to complete a unique CLI command fragment using the keyboard spacebar.

Syntax

set cli completion {**enable** | **disable**} [**default**]

Parameters

enable | **disable**	Enables or disables the CLI command completion function.
default	(Optional) Maintains the status for all future sessions.

Defaults

If not specified, the status setting will not be maintained as the default.

Mode

Switch command, Read-Write.

Example

This example shows how to enable the CLI command completion function and maintain it as the default setting:

```
Matrix(rw)->set cli completion enable default
```

loop

Use this command to execute a command loop.

Syntax

loop *count* [*delay*] [**-r**]

Downloaded from www.Manualslib.com manuals search engine

Parameters

count	Specifies the number of times to loop. A value of 0 will make the command loop forever.
delay	(Optional) Specifies the number of seconds to delay between executions.
-r	(Optional) Refreshes the cursor to the home position on the screen.

Defaults

- If a *delay* is not specified, none will be set.
- If not specified, the cursor will not refresh.

Mode

Switch command, Read-Write.

Example

This example shows how to execute a command loop 10 times with a 30 second delay:

```
Matrix(rw)->loop 10 30
```

show banner

Use this command to show the banner message that will display at pre and post session login.

Syntax

show banner {**login** | **motd**}

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Only.

Example

This example shows how to display the banner message of the day:

```
Matrix(rw)->show banner motd
Not one hundred percent efficient, of course ... but nothing ever is.
                -- Kirk, "Metamorphosis", stardate 3219.8
```


Downloaded from www.Manualslib.com manuals search engine

set banner

Use this command to set the banner message for pre and post session login.

Syntax

set banner {**login** *message* | **motd** *message*}

Parameters

login message	Specifies a message displayed pre session login. This is a text string that can be formatted with tabs (**\t**) and new line escape (**\n**) characters. The \t tabs will be converted into 8 spaces in the banner output.
motd *message*	Specifies a message of the day displayed post session login. This is a text string that can be formatted with tabs (**\t**) and new line escape (**\n**) characters. The \t tabs will be converted into 8 spaces in the banner output.

Defaults

None.

Mode

Switch command, Read-Write.

Usage

Use the **\?** escape sequence when ending a banner with a question mark to avoid the question mark being treated as a help request.

A pre-session login banner will cause a prompt to display when logging on to the system requiring the user to verify y/n before the login will continue. For example if the banner login is "By proceeding with this login you are verifying that you are a member of the Enterasys documentation group and are authorized to use this system." The following will display prior to entering the login password:

```
By proceeding with this login you are verifying that you are a member of the
Enterasys documentation group and are authorized to use this system.
Proceed to login? (y/n) [n]?
```

Examples

This example shows how to set the post session message of the day banner to read "Change is the price of survival.
-- Winston Churchill" :

```
Matrix(rw)->set banner motd Change is the price of survival. \n\t--Winston
Churchill
```

This example shows how to set the pre session message to read "There is nothing more important than our customers." :

```
Matrix(rw)->set banner login There is nothing more important than our customers
```


Downloaded from www.Manualslib.com manuals search engine

clear banner

Use this command to clear the banner message displayed at pre and post session login to a blank string.

Syntax

clear banner {**login** | **motd**}

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to clear the post session message of the day banner to a blank string:

```
Matrix(rw)->clear banner motd
```

show version

Use this command to display hardware and firmware information. Refer to "Downloading a New Firmware Image" on page 2-72 for instructions on how to download a firmware image.

Syntax

show version

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Only.

Example

This example shows how to display version information:

```
Matrix(rw)->show version
Copyright (c) 2004 by Enterasys Networks, Inc.

Slot    Model             Serial #              Versions
------  ----------------  --------------------  -------------
1       7G4270-12         CH-2R72               Hw: 2
```


Downloaded from www.Manualslib.com manuals search engine

```
                                                Bp: 01.00.10
                                                Fw: 05.01.56
2       7G4202-30         GR-A13                Hw: 0
                                                Bp: 01.00.05
                                                Fw: 05.01.56
3       7G4202-30         gr-a5                 Hw: 0
                                                Bp: 01.00.10
                                                Fw: 05.01.56
4       7G4202-30         GR-R18                Hw: 0
                                                Bp: 01.00.05
                                                Fw: 05.01.56
5       7K4290-02         040802623111          Hw: 2
                                                Bp: 01.00.15
                                                Fw: 05.01.56
6       7H4382-49         TRI_RA110             Hw: 3
                                                Bp: 01.00.10
                                                Fw: 05.01.56
7       7H4203-72         CP-22                 Hw: 0
                                                Bp: 01.00.09
                                          Fw: 05.01.561       4G4202-60
041405833244          Hw: 0
                                                Bp: 01.00.15
                                                Fw: 05.01.57

2       4H4282-49         03320004320A          Hw: 0
                                                Bp: 01.00.15
                                                Fw: 05.01.511        2G4072-52
       041405833244          Hw: 0
                                                Bp: 01.00.15
                                                Fw: 05.01.57
```

Table 2-6 provides an explanation of the command output.

Table 2-6 show version Output Details

Output...	What it displays...
Slot	Slot location designation. For details on how slots are numbered, refer to “Port String Syntax Used in the CLI” on page 4-2.
Model	Device’s model number.
Serial #	Device’s serial number of the device.
Versions	• **Hw**: Hardware version number. • **Bp**: BootPROM version • **Fw**: Current firmware version number.

Downloaded from www.Manualslib.com manuals search engine

set system name

Use this command to configure a name for the system.

Syntax

set system name [*string*]

Parameters

string	(Optional) Specifies a text string that identifies the system. **Note:** A name string containing a space in the text must be enclosed in quotes as shown in the example below.

Defaults

If *string* is not specified, the system name will be cleared.

Mode

Switch command, Read-Write.

Example

This example shows how to set the system name to Information Systems:

```
Matrix(rw)->set system name "Information Systems"
```

set system location

Use this command to identify the location of the system.

Syntax

set system location [*string*]

Parameters

string	(Optional) Specifies a text string that indicates where the system is located. **Note:** A location string containing a space in the text must be enclosed in quotes as shown in the example below.

Defaults

If *string* is not specified, the location name will be cleared.

Mode

Switch command, Read-Write.

Example

This example shows how to set the system location string:

```
Matrix(rw)->set system location "Bldg N32-04 Closet 9"
```


Downloaded from www.Manualslib.com manuals search engine

set system contact

Use this command to identify a contact person for the system.

Syntax

set system contact [*string*]

Parameters

string	(Optional) Specifies a text string that contains the name of the person to contact for system administration. **Note:** A contact string containing a space in the text must be enclosed in quotes as shown in the example below.

Defaults

If *string* is not specified, the contact name will be cleared.

Mode

Switch command, Read-Write.

Example

This example shows how to set the system contact string:

```
Matrix(rw)->set system contact "Joe Smith"
```

set width

Use this command to set the number of columns for the terminal connected to the device's console port. The length of the CLI is set using the **set length** command as described in "set length" on page 2-52.

Syntax

set width *screenwidth*

Parameters

screenwidth	Sets the number of terminal columns. Valid values are **50** to **150**.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to set the terminal columns to 50:

```
Matrix(rw)->set width 50
```


Downloaded from www.Manualslib.com manuals search engine

set length

Use this command to set the number of lines the CLI will display.

Syntax

set length *screenlength*

Parameters

screenlength	Sets the number of lines in the CLI display. Valid values are **0**, which disables the scrolling screen feature described in "Displaying Scrolling Screens" on page 2-10, and from **5** to **512**.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to set the terminal length to 50:

```
Matrix(rw)->set length 50
```

show logout

Use this command to display the time (in seconds) an idle console or Telnet CLI session will remain connected before timing out.

Syntax

show logout

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Only.

Example

This example shows how to display the CLI logout setting:

```
Matrix(rw)->show logout
Logout currently set to: 10 minutes.
```


Downloaded from www.Manualslib.com manuals search engine

set logout

Use this command to set the time (in minutes) an idle console or Telnet CLI session will remain connected before timing out.

Syntax

set logout *timeout*

Parameters

timeout	Sets the number of minutes the system will remain idle before timing out.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to set the system timeout to 10 minutes:

```
Matrix(rw)->set logout 10
```

show physical alias

Use this command to display the alias, a text name, for one or more physical objects.

Syntax

show physical alias [**chassis**] | [**slot** *slot*] | [**backplane** *backplane*] | [**module** *module*] | [**powersupply** *powersupply*] | [**powersupply-slot** *powersupply-slot*] | [**fan**] | [**fan-slot**] | [**port-string** *port-string*]

Parameters

chassis	(Optional) Displays the alias set for the chassis.
slot *slot*	(Optional) Displays the alias set for a specified slot in the chassis.
backplane *backplane*	(Optional) Displays the alias set for the backplane. Valid values are **1** for FTM 1 and **2** for FTM 2.
module *module*	(Optional) Displays the alias set for a specified module. A maximum of one module alias per slot is allowed.
powersupply *powersupply*	(Optional) Displays the alias set for a specified power supply. Valid values are **1** or **2**.
powersupply-slot *powersupply-slot*	(Optional) Displays an alias set for a specific power supply slot.
fan	(Optional) Displays the alias set for the fan tray.

Downloaded from www.Manualslib.com manuals search engine

fan-slot	(Optional) Displays an alias for the fan tray's slot.
port-string *port-string*	(Optional) Displays the alias set for a specified *port-string*. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.

Defaults

If no parameters are specified, all physical alias information will be displayed.

Mode

Switch command, Read-Only.

Example

This example shows how to display physical alias information for the chassis. In this case, the chassis entity is 1 and there is no alias currently set for the chassis:

```
Matrix(rw)->show physical alias chassis
chassis-1           alias=<empty string> entity=1
```

set physical alias

Use this command to set the alias, a text name, for a physical object.

Syntax

set physical alias {[**chassis**] [**slot** *slot*] [**backplane** *backplane*] [**module** *module*] [**powersupply** *powersupply*] [**powersupply-slot** *powersupply-slot*] [**fan**] [**fan-slot**] [**port-string** *port-string*]} [*string*]

Parameters

chassis	Sets an alias for the chassis.
slot *slot*	Sets an alias for a specific slot in the chassis.
backplane *backplane*	Sets an alias for the backplane. Valid values are **1** for FTM 1 and **2** for FTM 2.
module *module*	Sets an alias for a specific module. A maximum of one module per slot is allowed.
powersupply *powersupply*	Sets an alias for a specific power supply. Valid values are **1** or **2**.
powersupply-slot *powersupply-slot*	Sets an alias for a specific power supply slot.
fan	Sets an alias for the fan tray.
fan-slot	Sets an alias for the fan tray's slot.
port-string *port-string*	Sets an alias for a specific port.
string	(Optional) Assigns a text string alias to the specified physical object.

Defaults

If *string* is not specified, the alias of the type specified will be cleared.

Downloaded from www.Manualslib.com manuals search engine

Mode

Switch command, Read-Write.

Example

This example shows how to set the alias for the chassis to “chassisone”:

```
Matrix(rw)->set physical alias chassis chassisone
```

clear physical alias

Use this command to reset the alias for a physical object to a zero-length string.

Syntax

clear physical alias {[**chassis**] [**slot** *slot*] [**backplane** *backplane*] [**module** *module*] [**powersupply** *powersupply*] [**powersupply-slot** *powersupply-slot*] [**fan**] [**fan-slot**] [**port-string** *port-string*]}

Parameters

chassis	Clears the chassis alias.
slot *slot*	Clears and alias for a specific slot.
backplane *backplane*	Clears and alias for a specific backplane. Valid values are **1** for FTM 1 and **2** for FTM 2.
module *module*	Clears an alias for a specific module.
powersupply *powersupply*	Clears an alias for a specific power supply. Valid values are **1** or **2**.
fan	Clears the fan tray alias
port-string *port-string*	Clears an alias for a specific port.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to set clear the alias set for the chassis:

```
Matrix(rw)->clear physical alias chassis
```

show physical assetid

Use this command to display the asset ID for a module.

Syntax

show physical assetid module *module*

Downloaded from www.Manualslib.com manuals search engine

Parameters

module *module*	Specifies the module for which to display an asset ID.

Defaults

None.

Mode

Switch command, Read-Only.

Example

This example shows how to display asset ID information for module 1. In this case, none has been configured:

```
Matrix(rw)->show physical assetid module 1
module-1            assetID=<empty string> entity=71
```

set physical assetid

Use this command to set the asset ID for a module.

Syntax

set physical assetid module *module string*

Parameters

module *module*	Sets an asset ID for a specific module.
string	Specifies the asset ID.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to set the asset ID information for module 1 to “dfe1”:

```
Matrix(rw)->set physical assetid module 1 dfe1
```

clear physical assetid

Use this command to reset the asset ID for a module to a zero-length string.

Syntax

clear physical assetid module *module*

Downloaded from www.Manualslib.com manuals search engine

Parameters

module *module*	Specifies the module for which to clear the asset ID.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to clear the asset ID for module 1:

```
Matrix(rw)->clear physical assetid module 1
```


Downloaded from www.Manualslib.com manuals search engine

Activating Licensed Features

In order to enable advanced features, such as redundant management, routing protocols, and extended ACLs on a Matrix Series device, you must purchase and activate a license key. If you have purchased a license, you can proceed to activate your license as described in this section. If you wish to purchase a license, contact Enterasys Networks Sales.

About Redundant Management on Matrix DFE-Gold Series Modules



Note: Interoperability of Matrix DFE-Gold Series modules is dependent upon module placement rules during installation in the chassis. For details on these rules and their effects on system management, refer to the Matrix DFE-Gold Series Installation Guide.

The DFE-Gold System Management Module (SMM) coordinates and controls the configuration of the entire chassis. By default, this is the module installed in slot 1. Access to the SMM is available through any console (COM) port on any module in the chassis. Only one CLI session can be active at any one time, and active status is granted to the first connection to any of the console ports.

In order to enable switch and routing redundancy on a Matrix DFE-Gold Series device, you must purchase and activate a license key. If you have purchased a redundancy license, you can proceed to activate it as described in this section. If you wish to purchase a redundancy license, contact Enterasys Networks Sales.

When a redundancy license key is purchased and activated as described in this section, redundancy can be configured on the module in slot 2 of the chassis. Then, in the event module 1 fails, module 2 will assume chassis management.

Purpose

To activate and verify licensed features.

Commands

For information about...	Refer to page...
set license	2-58
show license	2-59
clear license	2-60

set license

When an advanced license is available, use this command to activate licensed features. If this is available on your Matrix Series device, a unique license key will display in the **show license** command output.

Syntax

set license {**advanced** | **redundancy**} *license-key* [**slot** *slot*]

Downloaded from www.Manualslib.com manuals search engine

Parameters

advanced	Activates advanced routing features.
redundancy	Activates management module redundancy.
license-key	Specifies your unique 16-digit hexadecimal advanced licensing key. **Note:** When available, the licensing key will display at the top of the **show running-config** command output.To see an example of this output, refer to "show running-config" on page 16-8.
slot *slot*	(Optional) Specifies a module to which the license will be bound.

Defaults

If not specified, the license will be bound to all modules.

Mode

Switch command, Read-Write.

Example

This example shows how to use license key abcdefg123456789 to activate advanced routing features:

```
Matrix(rw)->set license advanced abcdefg123456789
```

show license

When available and activated, use this command to display your license key.

Syntax

show license

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to display your license key information:

```
Matrix(rw)->show license
advanced abcdefg123456789
```


Downloaded from www.Manualslib.com manuals search engine

clear license

Use this command to clear license key settings.

Syntax

clear license {**advanced** | **redundancy**} [**slot** *slot*]

Parameters

advanced	Clears the advanced routing license setting.
redundancy	Clears the management module redundancy license setting.
slot *slot*	(Optional) Specifies a module from which the license setting will be cleared.

Defaults

If not specified, the license settings will be cleared from all modules.

Mode

Switch command, Read-Write.

Example

This example shows how to clear advanced license key settings:

```
Matrix(rw)->clear license advanced
```


Downloaded from www.Manualslib.com manuals search engine

Configuring Power over Ethernet (PoE)

Important Notice

This section applies only to PoE-equipped Matrix devices. Consult the Installation Guide shipped with your product to determine if it is PoE-equipped.

Purpose

To review and set PoE parameters, including the power available to the chassis, the usage threshold for each module, whether or not SNMP trap messages will be sent when power status changes, and per-port PoE settings.

Commands

For information about...	Refer to page...
show inlinepower	2-61
set inlinepower mode	2-62
clear inlinepower mode	2-63
set inlinepower available	2-63
clear inlinepower available	2-64
set inlinepower powertrap	2-65
clear inlinepower powertrap	2-65
set inlinepower assigned	2-66
clear inlinepower assigned	2-66
set inlinepower threshold	2-67
clear inlinepower threshold	2-67
set inlinepower management	2-68
clear inlinepower management	2-68
set inlinepower psetrap	2-69
clear inlinepower psetrap	2-69
show port inlinepower	2-70
set port inlinepower	2-70
clear port inlinepower	2-71

show inlinepower

Use this command to display device PoE properties.

Syntax

```
show inlinepower
```


Downloaded from www.Manualslib.com manuals search engine

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Only.

Example

This example shows how to display device PoE properties. In this case, only the modules in slots 2 and 3 are PoE modules, so their power configurations display:

```
Matrix(rw)->show inlinepower
Total Power Detected    : 1200 Watts
Total Power Available   : 1200 Watts (100% of Total Power Detected)
Total Power Assigned    : 0 Watts
Power Allocation Mode   : auto
Power Trap Status       : disabled
Power Redundancy Status : not redundant
Power Supply 1 Status   : installed and operating
Power Supply 2 Status   : not installed
Power Supply 3 Status   : not installed
Power Supply 4 Status   : not installed

Slot Oper   Power Power    Power     Class  Power Usage Usage PSE      Mgmt
     Status Limit Assigned Available Budget Usage       Trhld Trap     Mode
            (W)   (W)      (W)       (W)    (W)   (%)   (%)   Status
---- ------ ----- -------- --------- ------ ----- ----- ----- -------- --------
1    on     806   0        598       12           2     75    disabled class
2    on     806   0        599              5     1     75    disabled real-time
3                0
4                0
5                0
6                0
7                0
```

set inlinepower mode

Use this command to set the chassis power allocation mode.

Syntax

set inlinepower mode {**auto** | **manual**}

Downloaded from www.Manualslib.com manuals search engine

Parameters

auto	Assigns automatic mode to chassis power allocation.
manual	Assigns manual mode to chassis power allocation. This setting allows the values configured with the **set inlinepower assigned** command ("set inlinepower assigned" on page 2-66) to be applied to PoE modules.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to set the chassis power allocation mode to manual:

```
Matrix(rw)->set inlinepower mode manual
```

clear inlinepower mode

Use this command to reset chassis power allocation to the default mode of auto.

Syntax

clear inlinepower mode

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to reset the chassis power allocation mode to auto:

```
Matrix(rw)->clear inlinepower mode
```

set inlinepower available

Use this command to set the percentage of total power available that a chassis can withdraw from the total power detected.

Syntax

set inlinepower available *max-percentage*

Downloaded from www.Manualslib.com manuals search engine

Parameters

max-percentage	Specifies the percentage of maximum power available. Valid values are **0** - **100**.

Defaults

None.

Mode

Switch command, Read-Write.

Usage

If the total power wattage value set with the **set inlinepower assigned** command ("set inlinepower assigned" on page 2-66) is greater that the maximum power percentage specified with this command, a warning will display. If the user opts to execute these parameters, a ratio of assigned power will be applied to each module. Refer to the **show inlinepower** output ("show inlinepower" on page 2-61) for a sample warning message.

Example

This example shows how to set the maximum inline power available to the chassis to 70 percent:

```
Matrix(rw)->set inlinepower available 70
```

clear inlinepower available

Use this command to reset the percentage of the total power available to a chassis to the default value of 100.

Syntax

clear inlinepower available

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to reset the maximum inline power available to the chassis to 100 percent:

```
Matrix(rw)->clear inlinepower available
```


Downloaded from www.Manualslib.com manuals search engine

set inlinepower powertrap

Use this command to disable or enable the sending of an SNMP trap message whenever the status of the chassis PoE power supplies or the PoE system redundancy changes.

Syntax

set inlinepower powertrap {**disable** | **enable**}

Parameters

disable | **enable**	Disables or enables a chassis power supplies trap messaging.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to enable a chassis power supplies trap:

```
Matrix(rw)->set inlinepower powertrap enable
```

clear inlinepower powertrap

Use this command to reset chassis power trap messaging back to the default state of disabled.

Syntax

clear inlinepower powertrap

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to reset chassis power trap messaging to disabled:

```
Matrix(rw)->clear inlinepower powertrap
```


Downloaded from www.Manualslib.com manuals search engine

set inlinepower assigned

Use this command to manually assign Power Sourcing Equipment (PSE) power to a module in the chassis.

Syntax

set inlinepower assigned *power-value slot-number*

Parameters

power-value	Specifies a power value in watts.
slot-number	Specifies a module slot location for the power assignment.

Defaults

None.

Mode

Switch command, Read-Write.

Usage

If the total power wattage value set with this command is greater that the maximum power percentage specified with the **set inlinepower available** command ("set inlinepower available" on page 2-63), a warning will display. If the user opts to execute these parameters, a ratio of assigned power will be applied to each module. Refer to the **show inlinepower** output ("show inlinepower" on page 2-61) for a sample warning message.

Example

This example shows how to assign 200 watts of power to the module in slot 1:

```
Matrix(rw)->set inlinepower assigned 200 1
```

clear inlinepower assigned

Use this command to clear the power value manually assigned to one or more modules.

Syntax

clear inlinepower assigned [*slot-number*]

Parameters

slot-number	(Optional) Clears the power assignment from a specific module.

Defaults

If *slot-number* is not specified, power value assignments will be cleared from all modules.

Mode

Switch command, Read-Write.

Downloaded from www.Manualslib.com manuals search engine

Example

This example shows how to clear power assignments to all modules in the chassis:

```
Matrix(rw)->clear inlinepower assigned
```

set inlinepower threshold

Use this command to set the PoE usage threshold on a specified module.

Syntax

set inlinepower threshold *usage-threshold module-number*

Parameters

usage-threshold	Specifies a PoE threshold as a percentage of total system power usage. Valid values are **1** - **99**.
module-number	Specifies the module on which to set the PoE threshold.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to set the PoE threshold to 50 on module 1:

```
Matrix(rw)->set inlinepower threshold 50 1
```

clear inlinepower threshold

Use this command to reset the PoE usage threshold on a specified module to the default value of 75 percent.

Syntax

clear inlinepower threshold *module-number*

Parameters

module-number	Specifies the module on which to reset the PoE threshold.

Defaults

None.

Mode

Switch command, Read-Write.

Downloaded from www.Manualslib.com manuals search engine

Example

This example shows how to reset the PoE threshold to 75 on module 1:

```
Matrix(rw)->clear inlinepower threshold 1
```

set inlinepower management

Use this command to set the PoE management mode on a specified module.

Syntax

set inlinepower management {**realtime** | **class**} *module-number*

Parameters

realtime	Manages power based on the actual power consumption of the ports.
class	Manages power based on the IEEE 802.3af definition of the class upper limit, except classes 0 and 4, for which the actual power consumption is used.
module-number	Specifies the module on which to set the PoE management mode.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to set the PoE management mode to “class” on module 1:

```
Matrix(rw)->set inlinepower management class 1
```

clear inlinepower management

Use this command to reset the PoE management mode on a specified module back to the default setting of “realtime”.

Syntax

clear inlinepower management *module-number*

Parameters

module-number	Specifies the module on which to reset the PoE management mode.

Defaults

None.

Mode

Switch command, Read-Write.

Downloaded from www.Manualslib.com manuals search engine

Example

This example shows how to reset the PoE management mode to "realtime" on module 1:

```
Matrix(rw)->clear inlinepower management 1
```

set inlinepower psetrap

Use this command to enable or disable the sending of an SNMP trap message for a module whenever the status of its ports changes, or whenever the module's PoE usage threshold is crossed.

Syntax

set inlinepower psetrap {**disable** | **enable**} *module-number*

Parameters

disable | **enable**	Disables or enables PoE trap messaging.
module-number	Specifies the module on which to disable or enable trap messaging.

Defaults

Disabled.

Mode

Switch command, Read-Write.

Usage

The module's PoE usage threshold must be set using the **set inlinepower threshold** command as described in "set inlinepower threshold" on page 2-67.

Example

This example shows how to enable PoE trap messaging on module 1:

```
Matrix(rw)->set inlinepower psetrap enable 1
```

clear inlinepower psetrap

Use this command to reset PoE trap messaging for a module back to default state of disabled.

Syntax

clear inlinepower psetrap *module-number*

Parameters

module-number	Specifies the module on which to clear PoE trap messaging.

Defaults

None.

Downloaded from www.Manualslib.com manuals search engine

Mode

Switch command, Read-Write.

Example

This example shows how to reset PoE trap messaging for module 1 to disabled:

```
Matrix(rw)->clear inlinepower psetrap 1
```

show port inlinepower

Use this command to display all ports supporting PoE.

Syntax

show port inlinepower [*port-string*]

Parameters

port-string	(Optional) Displays information for specific PoE port(s).

Defaults

If not specified, information for all PoE ports will be displayed.

Mode

Switch command, Read-Only.

Example

This example shows how to display PoE information for Fast Ethernet ports 11, 12 and 13 in module 1:

```
Matrix(rw)->show port inlinepower fe.1.1-2
                      Oper             Admin                  Power Power PD
Port    Type          Status           Status Priority Class Limit Usage Type
        (truncated)                                           (mW)  (mW)
------- ------------- ---------------- ------ -------- ----- ----- ----- ------
fe.1.11 Wireless 1    delivering power auto   critical 0     16800 7500  legacy
fe.1.12 Wireless 2    delivering power auto   high     1     16800 7500  802.3af
fe.1.13 Wireless 3    searching        auto   low      3     16800 7500  other
```

set port inlinepower

Use this command to configure PoE parameters on one or more ports.

Syntax

set port inlinepower *port-string* {[**admin** {**off** | **auto**}] [**priority** {**critical** | **high** | **low**}] [**type** *type*] [**powerlimit** *powerlimit*]}

Downloaded from www.Manualslib.com manuals search engine

Parameters

port-string	Specifies the port(s) on which to configure PoE.
admin off | **auto**	Sets the PoE administrative state to off (disabled) or auto (on).
priority critical | **high** | **low**	Sets the port(s) priority for the PoE allocation algorithm to critical (highest), high or low.
type *type*	Specifies a string describing the type of device connected to a port.
powerlimit *powerlimit*	Sets the maximum power allowed on this port in megawatts. Valid values are 0 - 15400.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to enable PoE on port fe.3.1 with critical priority:

```
Matrix(rw)->set port inlinepower fe.3.1 admin auto priority critical
```

clear port inlinepower

Use this command to reset PoE parameters on one or more ports to default values.

Syntax

clear port inlinepower *port-string* {[**admin**] [**priority**] [**type**] [**powerlimit**]}

Parameters

port-string	Specifies the port(s) on which to reset PoE.
admin	Resets the PoE administrative state to **auto** (on).
priority	Resets the port(s) priority for the PoE allocation algorithm to **low**.
type	Resets the port type to an empty string.
powerlimit	Resets the maximum power to 15400 megawatts.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to rest the PoE priority on port fe.3.1 to low:

```
Matrix(rw)->clear port inlinepower fe.3.1 priority
```


Downloaded from www.Manualslib.com manuals search engine

Reviewing and Selecting a Boot Firmware Image

Downloading a New Firmware Image

You can upgrade the operational firmware in the Matrix Series device without physically opening the device or being in the same location. There are three ways to download firmware to the device:

- Via FTP download. This procedure uses an FTP server connected to the network and downloads the firmware using the FTP protocol. It is the most robust downloading mechanism. For details on how to perform an FTP download using the **copy** command, refer to "copy" on page 2-86.
- Via TFTP download. This procedure uses a TFTP server connected to the network and downloads the firmware using the TFTP protocol. For details on how to perform a TFTP download using the **copy** command, refer to "copy" on page 2-86.
- Via the serial (console) port. This procedure is an out-of-band operation that copies the firmware through the serial port to the device. It takes approximately five minutes and requires minimal configuration. It should be used in cases when you cannot connect the device to perform the in-band **copy** download procedure via FTP or TFTP. Serial console download has been successfully tested with the following applications:
  - HyperTerminal Copyright 1999
  - Tera Term Pro Version 2.3

Any other terminal applications may work but are not explicitly supported. For details, refer to "Downloading via the Serial Port" on page 2-72.

Important Notice

The Matrix Series device allows you to download and store multiple image files. This feature is useful for reverting back to a previous version in the event that a firmware upgrade fails to boot successfully. After downloading firmware as described above, you can select which image file you want the device to load at startup using the **setboot** command in the System Image Loader menu ("Downloading via the Serial Port" on page 2-72) or the **set boot system** command ("set boot system" on page 2-75).

Downloading from an FTP or TFTP Server

To perform an FTP or TFTP download, proceed as follows:

1. If you have not already done so, set the device's IP address using the **set ip address** command as detailed in "set ip address" on page 2-31.
2. Download a new image file using the **copy** command as detailed in "copy" on page 2-86.

You can now set the device to load the new image file at startup using the **set boot system** command as described in "set boot system" on page 2-75.

Downloading via the Serial Port

To download device firmware via the serial (console) port, proceed as follows:

1. With the console port connected, power up the device. The following message displays:

```
Boot ROM Initialization, Version 01.00.01

Copyright (c) 2004 Enterasys Networks, Inc.

SDRAM size: 128 MB
```


Downloaded from www.Manualslib.com manuals search engine

```
Testing SDRAM....                       PASSED.
Loading Boot Image: 01.00.02...         DONE.

Uncompressing Boot Image...             DONE.

Press any key to enter System Image Loader menu
```

2. Before the boot up completes, press any key. The following boot menu options screen displays.

```
Options available
1  - Start operational code
2  - Change baud rate
3  - Retrieve event log using XMODEM (64KB).
4  - Load new operational code using XMODEM
5  - Display operational code vital product data
6  - Run Flash Diagnostics
7  - Update Boot Code
8  - Delete operational code
9  - Reset the system
10 - Restore Configuration to factory defaults (delete config files)
```

3. Type **2**. The following baud rate selection screen displays:

```
1 - 1200
2 - 2400
3 - 4800
4 - 9600
5 - 19200
6 - 38400
7 - 57600
8 - 115200
0 - no change
```

4. Type **8** to set the device baud rate to 115200. The following message displays:

```
Setting baud rate to 115200, you must change your terminal baud rate.
```

5. Set the terminal baud rate to **115200** and press ENTER.
6. Type **download** to start the ZMODEM receive process.
7. Send the image file using the ZMODEM protocol from your terminal application. (This procedure will vary depending on your application.) When the ZMODEM download is finished, the following message displays:

```
[System Image Loader]: download
Preparing to receive file...

Writing file...
Download successful.
[System Image Loader]:
```

8. Set the device baud rate back to **9600.**

Downloaded from www.Manualslib.com manuals search engine

9. Set the terminal baud rate back to **9600** and press ENTER.
10. Type **setboot** *filename* to set the device to boot to the new firmware image. In this example, the downloaded image file is named "myimage." The following message displays:

```
[System Image Loader]: setboot myimage
Image boot file set to myimage
[System Image Loader]:
```

11. Type **boot** to reboot the device. The following message indicates the downloaded image booted successfully:

```
[System Image Loader]: boot
/flash0/  - Volume is OK
Loading myimage...                    DONE.
```



Note: If you reboot without specifying the image to boot with **setboot** as described above, the device will attempt to load whatever image is currently stored in the bootstring via the **set boot system** command ("set boot system" on page 2-75). If the device cannot find the image, or it is not set, it will search through available images and attempt to boot the newest one. It will then set the bootstring to whatever image file name was successfully loaded.

Purpose

To display and set the image file the device loads at startup.

Commands

For information about...	Refer to page...
show boot system	2-74
set boot system	2-75

show boot system

Use this command to display the firmware image the system will load at the next system reset.

Syntax

show boot system

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Only.

Downloaded from www.Manualslib.com manuals search engine

Usage

The system must be reset by software for the new boot image to take effect at startup. If the chassis is powered OFF and then back ON, the current active image will just reload at startup.

The **dir** command, as described in "dir" on page 2-81, displays additional information about boot image files. "Active" indicates the image that is currently running, and "Boot" means indicates the image that is currently scheduled to boot next. The **set boot system** command ("set boot system" on page 2-75) will move the boot designation from the current running image, but will allow the active image to stay where it is until after the reset, when that image has actually been booted.

Example

This example shows how to display the switch's boot firmware image:

```
Matrix(rw)->show boot system
Current system image to boot: bootfile
```

set boot system

Use this command to set the firmware image the switch loads at startup.

Syntax

set boot system *filename*

Parameters

filename	Specifies the name of the firmware image file.

Defaults

None.

Mode

Switch command, Read-Write.

Usage

This is the image that will be loaded automatically after the system has been reset. Although it is not necessary to choose to reset the system and activate the new boot image immediately, the CLI will prompt you whether or not you want to do so. You can choose "Yes" at the question prompt to have the system reset and load the new boot image immediately, or choose "No" to load the new boot image at a later scheduled time by issuing one of the following commands: **clear config**, **reset**, or **configure**. The new boot setting will be remembered through resets and power downs, and will not take effect until the **clear config**, **reset**, or **configure** command is given.

Example

This example shows how to set the boot firmware image file to "newimage" and reset the system with the new image loaded immediately:

```
Matrix(rw)->set boot system newimage
This command can optionally reset the system to boot the new image.
Do you want to reset now (y/n) [n]?y
Resetting system ...
```


Downloaded from www.Manualslib.com manuals search engine

Starting and Configuring Telnet

Purpose

To enable or disable Telnet, and to start a Telnet session to a remote host. The Matrix Series device allows a total of four inbound and / or outbound Telnet session to run simultaneously.

Commands

The commands used to enable, start and configure Telnet are listed below and described in the associated section as shown.

For information about...	Refer to page...
show telnet	2-76
set telnet	2-77
telnet	2-77
show router telnet	2-78
set router telnet	2-78
clear router telnet	2-79

show telnet

Use this command to display the status of Telnet on the device.

Syntax

show telnet

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Only.

Example

This example shows how to display Telnet:

```
Matrix(rw)->show telnet  status

Telnet inbound is currently: ENABLED
Telnet outbound is currently: ENABLED
```


Downloaded from www.Manualslib.com manuals search engine

set telnet

Use this command to enable or disable Telnet on the device.

Syntax

set telnet {**enable** | **disable**}{**inbound** | **outbound** | **all**}

Parameters

enable | **disable**	Enables or disables Telnet services.
inbound | **outbound** | **all**	Specifies inbound service (the ability to Telnet to this device), outbound service (the ability to Telnet to other devices), or all (both inbound and outbound).

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to disable inbound and outbound Telnet services:

```
Matrix(rw)->set telnet disable all

Disconnect all telnet sessions and disable now (y/n)? [n]: y
All telnet sessions have been terminated, telnet is now disabled.
```

telnet

Use this command to start a Telnet connection to a remote host. The Matrix Series device allows a total of four inbound and / or outbound Telnet session to run simultaneously.

Syntax

telnet *host* [*port*]

Parameters

host	Specifies the name or IP address of the remote host.
port	(Optional) Specifies the server port number.

Defaults

If not specified, the default *port* number 23 will be used.

Mode

Switch command, Read-Write.

Downloaded from www.Manualslib.com manuals search engine

Example

This example shows how to start a Telnet session to a host at 10.21.42.13:

```
Matrix(rw)->telnet 10.21.42.13
```

show router telnet

Use this command to display the state of Telnet service to the router.

Syntax

show router telnet

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Only.

Example

This example shows how to display the state of Telnet service to the router:

```
Matrix(rw)->show router telnet
Telnet to Router IP is enabled
```

set router telnet

Use this command to enable or disable Telnet service to the router interface IP address.

Syntax

set router telnet {**enable** | **disable**}

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to disable Telnet service to the router:

```
Matrix(rw)->set router telnet disable
```


Downloaded from www.Manualslib.com manuals search engine

clear router telnet

Use this command to reset Telnet service to the router to the default state of disabled.

Syntax

```
clear router telnet
```

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to reset Telnet service to the router:

```
Matrix(rw)->clear router telnet to disabled
```


Downloaded from www.Manualslib.com manuals search engine

Managing Configuration and Image Files

Matrix Series devices provide a single configuration interface which allows you to perform both switch and router configuration with the same command set. The device also provides redundant, distributed copies of each image file in the event that DFE modules are added or removed from the Matrix chassis. When managing configuration and image files on the Matrix Series device, it is important to remember the following considerations:

- All modules will have the same image files loaded. If a module is inserted into a chassis, any images unique to that module will be deleted, and any images not on that module will be copied to it.
- Configuration files are stored per slot, with each slot in the chassis carrying unique files with it and not inheriting files.

The Matrix Series devices now support a script feature that allows you to execute a previously created script file containing CLI commands, and at the time of execution, enter optional arguments that modify the actions of the commands. This feature is intended to simplify the configuration of ports and VLANs, by creating script files containing groups of commands that you want to run on the same port-string or VLAN id. At the time of execution, you pass in the port-string, VLAN id, and any other required arguments that you want the commands to operate on. Refer to the **script** command, "script" on page 2-88.

The following section describes the command set for managing both switch and router configuration.

For details on performing a basic routing configuration (while operating in router mode), refer to "Performing a Basic Router Configuration" on page 16-11.

For details on downloading a new firmware image, refer to "Downloading a New Firmware Image" on page 2-72.

For details on reviewing and selecting the boot firmware image, refer to "Reviewing and Selecting a Boot Firmware Image" on page 2-72.



Note: The commands described in this section manage both switch and router configuration parameters, but must be executed from the switch CLI.

Purpose

To view, manage, and execute configuration and image files.

Commands

For information about...	Refer to page...
dir	2-81
show file	2-83
show config	2-85
configure	2-86
copy	2-86
delete	2-87
script	2-88

Downloaded from www.Manualslib.com manuals search engine

dir

Use this command to list files stored in the file system.

Syntax

dir [*filename*]

Parameters

filename	(Optional) Specifies the file name or directory to list.

Defaults

If *filename* is not specified, all files in the system will be displayed.

Mode

Switch, Read-Only.

Example

This example shows how to list all the files in the system:

```
Matrix(rw)->dir
Images:
============================================================
Filename:      ets-mtxe7-msi
Version:       01.02.00
Size:          3263043 (bytes)
Date:          MON FEB 24 14:07:08 2003
CheckSum:      6a2398391ba885531f96f19e161b096b
Location:      slot3, slot4, slot5, slot6
Compatibility: 4H4282-49, 4H4283-49, 4H4203-72

Filename:      01_02_00 (Active) (Boot)
Version:       01.03.00
Size:          3293059 (bytes)
Date:          TUE MAR 04 06:18:22 2003
CheckSum:      77481f78b8963675e1ed48e5a0085513
Location:      slot3, slot4, slot5, slot6
Compatibility: 4H4282-49, 4H4283-49, 4H4203-72

Files:
=====================================================
slot3:

slot4:

slot5:
FEB 24 2003  15:25:24            7060 sample.cfg
```


Downloaded from www.Manualslib.com manuals search engine

```
slot6:


Filename:       04.21.03 (Active) (Boot)
Version:        04.21.03
Size:           5494579 (bytes)
Date:           FRI JUL 30 08:50:40 2004
CheckSum:       f564c266c3a5907a9f3750dd17db6999
Location:       slot1
Compatibility: 7G4202-30, 7G4202-60, 7G4270-09, 7G4270-10,                7G4270-
12, 7G4282-41, 7H4202-72, 7H4203-72,                7H4284-49, 7H4382-25, 7H4382-
49, 7H4383-49,                7H4385-49, 7K4290-02, 2G4072-52
Files:
=====================================================
slot1:
FEB 24 2004 15:25:24            7060 sample.cfg
```

Table 2-7 provides an explanation of the command output.

Table 2-7 dir Output Details

Output...	What it displays...
Images	Lists all the images resident in the chassis and information about each.
Filename	Name of the image file stored in the local file system. Various flags may be listed after the filename, including: • (active) - Indicates this image is currently running. • (boot) - Indicates this image is selected to boot on the next reset.
Version	Firmware version of the image.
Size	Size of image file in the local file system.
Date	Date of image file in the local file system.
CheckSum	MD5 checksum calculated across the entire image file, used for image identity and verification.
Location	Modules on which this image resides. The system automatically mirrors all images to all other compatible modules in the system. A user cannot selectively add or remove images from individual modules while they reside in the same chassis.
Compatibility	Module types on which this image is qualified to run. Attempting to run an incompatible image on a given module will not succeed.
Files	User maintained files, such as CLI configuration files. For details on working with configuration files, refer to **show config** (“show config” on page 2-85) and **configure** (“configure” on page 2-86.)
SlotN	Lists user maintained files by slot location.

Downloaded from www.Manualslib.com manuals search engine

show file

Use this command to display the contents of an image or configuration file.

Syntax

show file *filename*

Parameters

filename	Specifies the filename to display.

Defaults

None.

Mode

Switch, Read-Only.

Example

This example (an excerpt of the complete output) shows how to display the contents of the sample.cfg configuration file:

```
Matrix(rw)->show file slot4/sample.cfg
begin
!
# ***** NON-DEFAULT CONFIGURATION *****
!
!
!
#  SLOT   TYPE
#  ___    _________________
!
#   1     4H4282-49
#   2     4H4282-49
#   3     4H4282-49
#   4
#   5
#   6
#   7
!
!
# Router instance Configuration
begin router


router

enable
```


Downloaded from www.Manualslib.com manuals search engine

```
config t
write file
exit
disable
exit
end router
# arp
!
# cdp
!
# console
!

begin
!
# ***** NON-DEFAULT CONFIGURATION *****
!
!
!
#  SLOT   TYPE
#  ___    _________________
!
#   1     7G4270-12
#   2
#   3     7H4382-49
#   4     7H4382-49
#   5     7H4382-49
#   6     7H4382-49
#   7     7H4382-49
!
!
# Router instance 3 Configuration
begin router

router

enable
config t
write file
exit
disable
exit
end router

# arp
```


Downloaded from www.Manualslib.com manuals search engine

```
!
# cdp
!
# console
!
```

show config

Use this command to display the system configuration or write the configuration to a file.

Syntax

show config [**all**] [*facility*] [**outfile** *outfile*]

Parameters

all	(Optional) Displays default and non-default configuration settings.
facility	(Optional) Displays the configuration for a specific facility.
outfile *outfile*	(Optional) Specifies a file in which to store the configuration.

Defaults

If no parameters are specified, only non-default system configuration settings will be displayed.

Mode

Switch, Read-Write.

Example

This example shows how to display the current non-default device configuration:

```
Matrix(su)->show config
This command shows non-default configurations only.
Use 'show config all' to show both default and non-default configurations.


begin
!
# ***** NON-DEFAULT CONFIGURATION *****
!
!
# Router Configuration
begin router

router

enable
config t
router id  2.2.2.2
```


Downloaded from www.Manualslib.com manuals search engine

```
 interface loopback 1
  ip address 2.2.2.2 255.255.255.255
  no shutdown
.
.
.
end
```

configure

Use this command to execute a previously downloaded configuration file stored on the device.

Syntax

configure *filename* [**append**]

Parameters

filename	Specifies the path and file name of the configuration file to execute.
append	(Optional) Executes the configuration as an appendage to the current configuration. This is equivalent to typing the contents of the config file directly into the CLI and can be used, for example, to make incremental adjustments to the current configuration.

Defaults

If **append** is not specified, the current running configuration will be replaced with the contents of the configuration file, which will require an automated reset of the chassis.

Mode

Switch, Read-Write.

Example

This example shows how to execute the “myconfig” file in the module in slot 1:

```
Matrix(rw)->configure slot1/myconfig
```

copy

Use this command to upload or download an image or a CLI configuration file.

Syntax

copy *source destination*

Downloaded from www.Manualslib.com manuals search engine

Parameters

source	Specifies location and name of the source file to copy. Options are a local file path (valid directories are /images and /slotN), or the URL of an FTP or TFTP server.
destination	Specifies location and name of the destination where the file will be copied. Options are a slot location and file name, or the URL of an FTP or TFTP server.

Defaults

None.

Mode

Switch, Read-Write.

Usage

The Matrix module to which a configuration file is downloaded must have the same hardware configuration as the Matrix module from which it was uploaded.

Examples

This example shows how to download an image via TFTP:

```
Matrix(rw)->copy tftp://134.141.89.34/ets-mtxe7-msi newimage
```

This example shows how to download an image via Anonymous FTP:

```
Matrix(rw)->copy ftp://134.141.89.34/ets-mtxe7-msi newimage
```

This example shows how to download an image via FTP with user credentials:

```
Matrix(rw)->copy ftp://user:passwd@134.141.89.34/ets-mtxe7-msi newimage
```

This example shows how to download a configuration file via TFTP to the slot 3 directory:

```
Matrix(rw)->copy tftp://134.141.89.34/myconfig slot3/myconfig
```

This example shows how to upload a configuration file via Anonymous FTP from the module in slot 3:

```
Matrix(rw)->copy slot3/myconfig ftp://134.141.89.34/myconfig
```

This example shows how to copy a configuration file from the slot 3 directory to the slot 5 directory:

```
Matrix(rw)->copy slot3/myconfig slot5/myconfig
```

delete

Use this command to remove an image or a CLI configuration file from the Matrix system.

Syntax

delete *filename*

Parameters

filename	Specifies the local path name to the file. Valid directories are /images and /slotN.

Downloaded from www.Manualslib.com manuals search engine

Defaults

None.

Mode

Switch, Read-Write.

Usage

Use the **show config** command as described in "show config" (page 2-85)to display current image and configuration file names.

Examples

This example shows how to delete the "myconfig" configuration file from slot 3:

```
Matrix(rw)->delete slot3/myconfig
```

This example shows how to delete the "010300" image file:

```
Matrix(rw)->delete images/010300
```

script

Use this command to execute a script file.

Syntax

script *filename* [*arg1*] [*arg2*] [*arg3*] [*arg4*] [*arg5*] [*arg6*] [*arg7*]

Parameters

filename	Specifies the local path name to the file. Valid directories are /images and /slotN.
arg1 through *arg7*	Specifies up to seven arguments to the script.

Defaults

None.

Mode

Switch, Read-Write.

Usage

The script file must first be created on a PC and copied to the Matrix device using the **copy** command ("copy" on page 2-86) before the script can be executed. The file can contain any number of switch commands, up to a maximum file size of 128 kilobytes. Router commands cannot be included in the file. Scripts cannot be nested within the file. Note that the **history** command will not reflect the execution of commands within a script file.

Example

This example uses the **copy** command to copy the script file named "setport.scr" from IP address 10.1.221.3 to slot 4. Next, the contents of the file is displayed with the **show file** command. The

Downloaded from www.Manualslib.com manuals search engine

script file requires two arguments, a port string (%1) and a VLAN id (%2). Finally, the script is executed, by specifying fe.1.1 as the first argument and 100 as the second argument.

```
Matrix(rw)->copy tftp://10.1.221.3/setport.scr slot4/setport.scr


Matrix(rw)->show file slot4/setport.scr
set port alias %1 script_set_port
set port vlan %1 %2 modify-egress
set port jumbo enable %1
set port disable %1
set port lacp port %1 disable


Matrix(rw)->script slot4/setport.scr fe.1.1 100
```

When the **script** command parses the file and performs the command line argument substitution, the commands are converted to the following:

```
set port alias fe.1.1 script_set_port
set port vlan fe.1.1 100 modify-egress
set port jumbo enable fe.1.1
set port disable fe.1.1
set port lacp port fe.1.1 disabled
```

The converted strings are then executed by the CLI engine and the **script** command returns.

Downloaded from www.Manualslib.com manuals search engine

Enabling or Disabling the Path MTU Discovery Protocol

Purpose

To enable or disable the path MTU (Maximum Transmission Unit) discovery protocol on the device. Because ports with transmission speeds higher than 100 Mbps are capable of transmitting frames up to a maximum of 10,239 bytes, it is necessary to have the path MTU discovery protocol enabled if jumbo frames are allowed in the network. If the system receives a frame larger than the destination port supports, it will send an "ICMP destination unreachable" error message indicating to the transmitting station that it must fragment the frame.



Note: By default, path MTU discovery is enabled on the device and jumbo frame support is disabled on all ports. When jumbo frame support is enabled with the **set port jumbo** command, as described in "set port jumbo" on page 4-28, path MTU discovery should not be disabled.

Commands

For information about...	Refer to page...
show mtu	2-90
set mtu	2-91
clear mtu	2-91

show mtu

Use this command to display the status of the path MTU discovery protocol on the device.

Syntax

```
show mtu
```

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Only.

Example

This example shows how to display path MTU discovery status:

```
Matrix(rw)->show mtu
MTU discovery status: Enabled
```


Downloaded from www.Manualslib.com manuals search engine

set mtu

Use this command to disable or re-enable path MTU discovery protocol on the device.

Syntax

set mtu {**enable** | **disable**}

Parameters

enable | **disable**	Enables or disables path MTU discovery protocol.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to disable path MTU discovery:

```
Matrix(rw)->set mtu disable
```

clear mtu

Use this command to reset the state of the path MTU discovery protocol back to enabled.

Syntax

clear mtu

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to reset the state of MTU discovery:

```
Matrix(rw)->clear mtu
```


Downloaded from www.Manualslib.com manuals search engine

Pausing, Clearing and Closing the CLI

Purpose

To clear the CLI screen or to close your CLI session.

Commands

The commands used to clear and close the CLI session are listed below and described in the associated sections as shown.

For information about...	Refer to page...
cls (clear screen)	2-92
exit | quit	2-92

cls (clear screen)

Use this command to clear the screen for the current CLI session.

Syntax

cls

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Only.

Example

This example shows how to clear the CLI screen:

```
Matrix(rw)->cls
```

exit | quit

Use either of these commands to leave a CLI session.

Syntax

exit

quit

Parameters

None.

Downloaded from www.Manualslib.com manuals search engine

Defaults

None.

Mode

Switch command, Read-Only.

Usage

By default, device timeout occurs after 15 minutes of user inactivity, automatically closing your CLI session. Use the **set logout** command as described in "set logout" on page 2-53 to change this default.

When operating in router mode, the **exit** command jumps to a lower configuration level. For details on enabling router configuration modes, refer to "Enabling Router Configuration Modes" on page 2-103.

Example

This example shows how to exit a CLI session:

```
Matrix(rw)->exit
```


Downloaded from www.Manualslib.com manuals search engine

Resetting the Device

Purpose

To reset one or more device modules, to clear the user-defined switch and router configuration parameters, or to schedule a system reset in order to load a new boot image.

Commands

The commands used to reset the device and clear the configuration are listed below and described in the associated sections as shown.

For information about...	Refer to page...
show reset	2-94
reset	2-95
reset at	2-96
reset in	2-96
clear config	2-97

show reset

Use this command to display information about scheduled device resets.

Syntax

show reset

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Only.

Example

This command shows how to display reset information

```
Matrix(rw)->show reset


Reset scheduled for Fri Jan 21 2000, 23:00:00 (in 3 days 12 hours 56 minutes 57
seconds).
Reset reason: Software upgrade
```


Downloaded from www.Manualslib.com manuals search engine

reset

Use this command to reset the device without losing any user-defined configuration settings

Syntax

reset {[*mod* | **system** | **nemcpu** {*mod.nemcpu*}] [**cancel**]}

Parameters

mod	Specifies a module to be reset.
system	Resets the system.
nemcpu *mod.nemcpu*	Resets the CPU on a Matrix Security Module or other processing NEM, where *mod* specifies the DFE module in which the Matrix Security Module or processing NEM is installed and *nemcpu* specifies the location of the NEM. Currently, this value can only be 1.
cancel	Cancels a reset scheduled using the **reset at** command as described in "reset at" on page 2-96, or the **reset in** command as described in "reset in" on page 2-96.

Defaults

None.

Mode

Read-Write.

Usage

A Matrix Series device can also be reset with the RESET button located on its front panel. For information on how to do this, refer to the *Matrix Installation Guide* shipped with your device.

Examples

This example shows how to reset the system.

```
Matrix(rw)->reset
 This command will reset the system and may disconnect your telnet session.
 Do you want to continue (y/n) [n]? y

 Resetting...
```

This example shows how to cancel a scheduled system reset:

```
Matrix(rw)->reset cancel

Reset cancelled.
```

This example shows how to reset a Matrix Security Module installed on the DFE in slot 4.

```
Matrix(rw)->reset nemcpu 4.1
This command will reset NEM CPU 4.1.
Do you want to continue (y/n) [n]? y
Resetting NEM CPU 4.1 ...
```


Downloaded from www.Manualslib.com manuals search engine

reset at

Use this command to schedule a system reset at a specific future time. This feature is useful for loading a new boot image.

Syntax

reset at *hh:mm* [*mm/dd*] [*reason*]

Parameters

hh:mm	Schedules the hour and minute of the reset (using the 24-hour system).
mm/dd	(Optional) Schedules the month and day of the reset.
reason	(Optional) Specifies a reason for the reset.

Defaults

- If month and day are not specified, the reset will be scheduled for the first occurrence of the specified time.
- If a *reason* is not specified, none will be applied.

Mode

Switch command, Read-Write.

Examples

Matrix(rw)->reset at 20:00 10/12This example shows how to schedule a reset at 8 p.m. on October 12:

```
Reset scheduled at 20:00:00, Sat Oct 12 2002
Proceed with scheduled reset? (y/n) [n]? y
Reset scheduled for 20:00:00, Sat Oct 12 2002 (in 1 day 5 hours 40 minutes
```

This example shows how to schedule a reset at a specific future time and include a reason for the reset:

```
Matrix(rw)->reset at 20:00 10/12 Software upgrade to 6.1(1)
Reset scheduled at 20:00:00, Sat Oct 12 2002
Reset reason: Software upgrade to 6.1(1)
Proceed with scheduled reset? (y/n) [n]? y
Reset scheduled for 20:00:00, Sat Oct 12 2002 (in 1 day 5 hours 40 minutes
```

reset in

Use this command to schedule a system reset after a specific time. This feature is useful for loading a new boot image.

Syntax

reset in *hh:mm* [*reason*]

Downloaded from www.Manualslib.com manuals search engine

Parameters

hh:mm	Specifies the number of hours and minutes into the future to perform a reset.
reason	(Optional) Specifies a reason for the reset

Defaults

If a *reason* is not specified, none will be applied.

Mode

Switch command, Read-Write.

Example

Matrix(rw)->reset in 5:20This example shows how to schedule a device reset in 5 hours and 20 minutes:

```
Reset scheduled in 5 hours and 20 minutes
Proceed with scheduled reset? (y/n) [n]? y
Reset scheduled for 19:56:01, Wed March 15 2002 (in 5 hours 20 minutes
```

clear config

Use this command to clear the user-defined switch and router configuration parameters for one or more modules.

Syntax

clear config *mod-num* | **all**

Parameters

mod-num | **all**	Clears configuration parameters in a specific module or in all modules.

Defaults

None.

Mode

Read-Write.

Usage

Executing clear config on one Matrix module resets that module back to its factory defaults. If that module is in a chassis with other active modules, it will inherit system settings from the system. For a list of factory device default settings, refer to "Factory Default Settings" on page 2-1.

This command will not affect the IP address.

Example

This example shows how to clear configuration parameters in all modules:

```
Matrix(rw)->clear config all
```


Downloaded from www.Manualslib.com manuals search engine

Gathering Technical Support Information

Purpose

To gather common technical support information.

Command

For information about...	Refer to page...
show support	2-98

show support

Use this command to display output for technical support-related commands.

Syntax

show support [*filename*]

Parameters

filename	(Optional) Filename (slotN/name) to save output.

Defaults

The following commands are executed:

- show version (“show version” on page 2-48)
- show system hardware (“show system hardware” on page 2-35)
- show vlan (“show vlan” on page 7-3)
- show vlan static (“show vlan” on page 7-3)
- show logging all (“show logging all” on page 10-2)
- show snmp counters (“show snmp counters” on page 5-6)
- show port status (“show port status” on page 4-14)
- show spantree status (“show spantree stats” on page 6-6)
- show spantree blockedports (“show spantree blockedports” on page 6-54)
- show ip address (“show ip address” on page 2-31)
- show ip route (“show ip route” on page 10-60)
- show netstat (“show netstat” on page 10-17)
- show arp (“show arp” on page 10-57)
- show system utilization (“show system utilization” on page 2-37)
- show config (“show config” on page 2-85)

Mode

Switch command, Read-Only.

Downloaded from www.Manualslib.com manuals search engine

Example

This example shows how to execute the **show support** command and save the results to slot 1 as a support3.txt file:

```
Matrix(su)->show support slot1/support3.txt
Writing output to file..................
Writing 'show config' output.....
Writing Message Log output.......
Matrix(su)->
```

There is no display example as the list of commands is quite lengthy. Click on the hyper-links in the “Command Defaults” section above, which contains a list of the individual commands executed, for more information and example outputs for the individual commands.

Downloaded from www.Manualslib.com manuals search engine

Preparing the Device for Router Mode

Important Notice

Startup and general configuration of the Matrix Series device must occur from the switch CLI. For details on how to start the device and configure general platform settings, refer to "Startup and General Configuration Summary" on page 2-1 and "Setting User Accounts and Passwords" on page 2-15. Once startup and general device settings are complete, IP configuration and other router-specific commands can be executed when the device is in router mode. For details on how to enable router mode from the switch CLI, refer to Table 2-9 in "Enabling Router Configuration Modes" on page 2-103.

For information about...	Refer to page...
Pre-Routing Configuration Tasks	2-100
Reviewing and Configuring Routing	2-101
Enabling Router Configuration Modes	2-103

Pre-Routing Configuration Tasks

The following pre-routing tasks, as detailed in "Startup and General Configuration Summary" on page 2-1 and "Setting User Accounts and Passwords" on page 2-15, must be performed from the switch CLI.

- Starting up the CLI. ("Starting and Navigating the Command Line Interface" on page 2-7)
- Setting the system password. ("set password" on page 2-18)
- Configuring basic platform settings, such as host name, system clock, and terminal display settings. ("Setting Basic Device Properties" on page 2-30)
- Setting the system IP address. ("set ip address" on page 2-31)
- Create and enable VLANs. (Chapter 7)
- File management tasks, including uploading or downloading flash or text configuration files, and displaying directory and file contents. ("Managing Configuration and Image Files" on page 2-80)

Note: The command prompts used as examples in Table 2-8 and throughout this guide show switch operation for a user in Read-Write (**rw**) access mode, and a system where module 1 and VLAN 1 have been configured for routing. The prompt changes depending on your current configuration mode, the specific Matrix device and module, and the interface types and numbers configured for routing on your system.

Table 2-8 Enabling the Switch for Routing

	To do this task	Type this command...	At this prompt...	For details see...
Step 1	Enable router mode.	**router**	Switch: **Matrix (rw)->**	"router" on page 2-103
Step 2	Enable router Privileged EXEC mode.	enable	Router: **Matrix>Router>**	"Enabling Router Configuration Modes" on page 2-103

Downloaded from www.Manualslib.com manuals search engine

Table 2-8 Enabling the Switch for Routing

	To do this task	Type this command...	At this prompt...	For details see...
Step 3	Enable global router configuration mode.	**configure terminal**	Router: **Matrix>Router#**	"Enabling Router Configuration Modes" on page 2-103
Step 4	Enable interface configuration mode using the interface of the routing module.	**interface** {**vlan** *vlan-id* | **loopback** *loopback-id*	Router: **Matrix> Router(config)#**	"interface" on page 16-3
Step 5	Assign an IP address to the routing interface.	**ip address** {*ip-address ip-mask*}	Router: **Matrix>Router (config-if (**Vlan 1 | Lpbk 1))#**	"ip address" on page 16-6
Step 6	Enable the interface for IP routing.	**no shutdown**	Router: **Matrix>Router (config-if (**Vlan 1 | Lpbk 1))#**	"no shutdown" on page 16-7

The example in Figure 2-8 shows how to:

- Enable routing for this router.
- Configure VLAN 1 on IP address 182.127.63.1 255.255.255.0 as the routing interface.

Figure 2-8 Enabling the Switch for Routing

```
Matrix(rw)->router
Matrix>router>enable
Matrix>router#configure terminal
 Enter configuration commands:
Matrix>Router(config)#interface vlan 1
Matrix>Router(config-if(Vlan 1))#ip address 182.127.63.1 255.255.255.0
Matrix>Router(config-if(Vlan 1))#no shutdown
```

Reviewing and Configuring Routing

Purpose

To review and configure routing.

Commands

For information about...	Refer to page...
show router	2-102
clear router	2-102
router	2-103

Downloaded from www.Manualslib.com manuals search engine

show router

Use this command to display which module that is currently running routing services. The DFE is a distributed system, which means that even though the protocols are running on a specific module, routing frames is done locally by every module.

Syntax

show router

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to display the module that is currently running routing services. :

```
Matrix(rw)->show router
Router Services are currently running on module 1
```

clear router

Use this command to clear the router configuration. This command de-configures the router and will remove the persistent router configuration. It will effectively write a blank configuration file to persistent memory. Before using this command, save the current configuration using the **show config** *outfile* command in "show config" on page 2-85.

Syntax

clear router

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to clear the router configuration:

```
Matrix(rw)->clear router
```


Downloaded from www.Manualslib.com manuals search engine

router

Use this command to enter router CLI mode.

Syntax

router

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to enable routing on this router:

```
Matrix(su)->router
Matrix(rw)->Router>
```

Enabling Router Configuration Modes

The Matrix CLI provides different modes of router operation for issuing a subset of commands from each mode. Table 2-9 describes these modes of operation.

Note: The command prompts used as examples in Table 2-9 and throughout this guide show switch operation for a user in Read-Write (**rw**) access mode, and a system where module 1 and VLAN 1 have been configured for routing. The prompt changes depending on your current configuration mode, the specific module, and the interface types and numbers configured for routing on your system.

Table 2-9 Router CLI Configuration Modes

Use this mode...	To...	Access method...	Resulting Prompt...
Privileged EXEC Mode	• Set system operating parameters • Show configuration parameters • Save/copy configurations	From the switch CLI: 1. Type **router**, then 2. Type **enable**.	**Matrix>Router>** **Matrix>Router#**
Global Configuration Mode	Set system-wide parameters.	Type **configure terminal** from Privileged EXEC mode.	**Matrix>router(config)#**
Interface Configuration Mode	Configure router interfaces.	Type **interface vlan** or **interface loopback** and the interface's *id* from Global Configuration mode.	**Matrix>router (config-if(Vlan 1** | Lpbk 1**))#**

Downloaded from www.Manualslib.com manuals search engine

Table 2-9 Router CLI Configuration Modes (continued)

Use this mode...	To...	Access method...	Resulting Prompt...
Router Configuration Mode	Set IP protocol parameters.	Type **router** and the *protocol name* (and, for OSPF, the *instance ID*) from Global or Interface Configuration mode.	**Matrix>router (config-router)#**
Key Chain Configuration Mode	Set protocol (RIP) authentication key parameters.	Type **key chain** and the key chain *name* from Router (RIP) Configuration mode.	Matrix>router (config-keychain)#
Key Chain Key Configuration Mode	Configure a specific key within a RIP authentication key chain.	Type **key** and the *key-id* from Key Chain Configuration Mode.	Matrix>router (config-keychain-key)#
Route Map Configuration Mode	Configure route maps 1-99.	Type **route-map**, an *id-number*, and **permit** or **deny** from Global Configuration Mode.	**Matrix>router (config-route-map)#**
Policy-Based Routing Configuration Mode	Configure policy-based routing for route maps 100-199.	Type **route-map**, an *id-number*, and **permit** or **deny** from Global Configuration Mode.	**Matrix>router (config-route-map-pbr)#**
Server Load Balancing (SLB) Server Farm Configuration Mode	Configure an LSNAT server farm.	Type **ip slb serverfarm** and the *serverfarmname* from Global Configuration Mode.	Matrix>router (config-slb-sfarm)#
Server Load Balancing (SLB) Real Server Configuration Mode	Configure an LSNAT real server.	Type **real** and the real server *IP address* from SLB Server Farm Configuration Mode.	Matrix>router (config-slb-real)#
Server Load Balancing (SLB) Virtual Server Configuration Mode	Configure an LSNAT virtual server.	Type **ip slb vserver** and the *vserver-name* from Global Configuration Mode.	Matrix>router (config-slb-vserver)#
IP Local Pool Configuration Mode	Configure a local address pool as a DHCP subnet	Type **ip local pool** and the local pool *name* from Global Configuration Mode.	Matrix>router (ip-local-pool)#
DHCP Pool Configuration Mode	Configure a DHCP server address pool.	Type **ip dhcp pool** and the address pool *name* from Global Configuration Mode.	Matrix>router (config-dhcp-pool)#
DHCP Class Configuration Mode	Configure a DHCP client class.	Type **client-class** and the client class *name* from DHCP Pool or Host Configuration Mode.	Matrix>router (config-dhcp-class)#

Downloaded from www.Manualslib.com manuals search engine

Table 2-9 Router CLI Configuration Modes (continued)

Use this mode...	To...	Access method...	Resulting Prompt...
DHCP Host Configuration Mode	Configure DHCP host parameters.	Type **client-identifier** and the *identifier*, or **hardware-address** and an *address* from any DHCP configuration mode.	Matrix>router (config-dhcp-host)#



Note: To jump to a lower configuration mode, type **exit** at the command prompt. To revert back to switch CLI, type **exit** from Privileged EXEC router mode.

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

3

Discovery Protocols Configuration

This chapter describes how to configure the discovery protocols supported by the firmware using CLI commands.

For information about...	Refer to page...
Displaying Neighbors	3-1
Enterasys Discovery Protocol	3-3
Cisco Discovery Protocol	3-8
Link Layer Discovery Protocol and LLDP-MED	3-15

Displaying Neighbors

Purpose

The show neighbors command displays neighbor discovered by all support discovery protocols.

Command

For information about...	Refer to page...
show neighbors	3-1

show neighbors

Use this command to display Network Neighbor Discovery information from all supported discovery protcols.

Syntax

show neighbors [*port-string*]

Parameters

port-string	(Optional) Displays Network Neighbor Discovery information for a specific port. For a detailed description of possible port-string values, refer to "Port String Syntax Used in the CLI" on page 4-2.

Downloaded from www.Manualslib.com manuals search engine

Defaults

If *port-string* is not specified, all Network Neighbor Discovery information will be displayed.

Mode

Switch command, Read-Only.

Example

This example shows how to display Network Neighbor Discovery information:

```
Matrix(rw)->show neighbors

Port       Device ID           Port ID             Type    Network Address
-------------------------------------------------------------------------------
fe.1.27    00-00-1d-83-77-3f   10.21.64.135        cdp     10.21.64.135
fe.1.33    00-e0-63-9d-c1-62   10.21.64.21         cdp     10.21.64.21
fe.1.34    00-01-f4-2a-c8-1f   10.21.70.1          cdp     10.21.70.1
fe.1.46    00-01-f4-00-73-00   ge.1.1              lldp    10.21.64.20
fe.1.47    00-01-f4-00-70-18   fe.1.10             lldp
fe.1.51    00-01-f4-00-7d-cc   10.21.65.129        cdp     10.21.65.129
fe.1.51    00-e0-63-86-47-53   10.21.65.128        cdp     10.21.65.128
fe.1.52    00e063d6892f        ge.1.1              ciscodp 10.21.85.10
fe.2.3     00e012345666        fe.1.3              ciscodp 10.21.64.60
```


Downloaded from www.Manualslib.com manuals search engine

Enterasys Discovery Protocol

Purpose

To enable and configure the Enterasys Discovery Protocol (CDP), used to discover network topology. When enabled, CDP allows Enterasys devices to send periodic PDUs about themselves to neighboring devices.

Commands

For information about...	Refer to page...
show cdp	3-3
set cdp state	3-4
set cdp auth	3-5
set cdp interval	3-6
set cdp hold-time	3-6
clear cdp	3-7

show cdp

Use this command to display the status of the CDP discovery protocol and message interval on one or more ports.

Syntax

show cdp [*port-string*]

Parameters

port-string	(Optional) Displays CDP status for a specific port. For a detailed description of possible port-string values, refer to "Port String Syntax Used in the CLI" on page 4-2.

Defaults

If *port-string* is not specified, all CDP information will be displayed.

Mode

Switch command, Read-Only.

Example

This example shows how to display CDP information for ports fe.1.1 through fe.1.9:

```
Matrix(rw)->show cdp fe.1.1-9
CDP Global Status         : enabled
CDP Versions Supported    : 0x0 0x38
CDP Hold Time             : 180
```


Downloaded from www.Manualslib.com manuals search engine

```
CDP Authentication Code  : 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0
0x0 0x0
CDP Transmit Frequency   : 60

Port       Status
-----------------
fe.1.1     auto-enable
fe.1.2     auto-enable
fe.1.3     auto-enable
fe.1.4     auto-enable
fe.1.5     auto-enable
fe.1.6     auto-enable
fe.1.7     auto-enable
fe.1.8     auto-enable
fe.1.9     auto-enable
```

Table 3-1 provides an explanation of the command output.

Table 3-1 show cdp Output Details

Output...	What it displays...
CDP Global Status	Whether CDP is globally auto-enabled, enabled or disabled. The default state of auto-enabled can be reset with the **set cdp state** command. For details, refer to "set cdp state" on page 3-4.
CDP Versions Supported	CDP version number(s) supported by the device.
CDP Hold Time	Minimum time interval (in seconds) at which CDP configuration messages can be set. The default of 180 seconds can be reset with the **set cdp hold-time** command. For details, refer to "set cdp hold-time" on page 3-6.
CDP Authentication Code	Authentication code for CDP discovery protocol. The default of 00-00-00-00-00-00-00-00 can be reset using the **set cdp auth** command. For details, refer to "set cdp auth" on page 3-5.
CDP Transmit Frequency	Frequency (in seconds) at which CDP messages can be transmitted. The default of 60 seconds can be reset with the **set cdp interval** command. For details, refer to "set cdp interval" on page 3-6.
Port	Port designation. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.
Status	Whether CDP is enabled, disabled or auto-enabled on the port.

set cdp state

Use this command to enable or disable the CDP discovery protocol on one or more ports.

Syntax

set cdp state {**auto** | **disable** | **enable**} [*port-string*]

Downloaded from www.Manualslib.com manuals search engine

Parameters

auto | **disable** | **enable**	Auto-enables, disables or enables the CDP protocol on the specified port(s). In auto-enable mode, which is the default mode for all ports, a port automatically becomes CDP-enabled upon receiving its first CDP message.
port-string	(Optional) Enables or disables CDP on specific port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.

Defaults

If *port-string* is not specified, the CDP state will be globally set.

Mode

Switch command, Read-Write.

Examples

This example shows how to globally enable CDP:

```
Matrix(rw)->set cdp state enable
```

This example shows how to enable the CDP for port fe.1.2:

```
Matrix(rw)->set cdp state enable fe.1.2
```

This example shows how to disable the CDP for port fe.1.2:

```
Matrix(rw)->set cdp state disable fe.1.2
```

set cdp auth

Use this command to set a global CDP authentication code.

Syntax

set cdp auth *auth-code*

Parameters

auth-code	Specifies an authentication code for the CDP protocol. This can be up to 16 hexadecimal values separated by commas.

Defaults

None.

Mode

Switch command, Read-Write.

Usage

This value determines a device's CDP domain. If two or more devices have the same CDP authentication code, they will be entered into each other's CDP neighbor tables. If they have different authentication codes, they are in different domains and will not be entered into each other's CDP neighbor tables.

Downloaded from www.Manualslib.com manuals search engine

A device with the default authentication code (16 null characters) will recognize all devices, no matter what their authentication code, and enter them into its CDP neighbor table.

Example

This example shows how to set the CDP authentication code to 1,2,3,4,5,6,7,8:

```
Matrix(rw)->set cdp auth 1,2,3,4,5,6,7,8
```

set cdp interval

Use this command to set the message interval frequency (in seconds) of the CDP discovery protocol.

Syntax

set cdp interval *frequency*

Parameters

frequency	Specifies the transmit frequency of CDP messages in seconds.Valid values are from **5** to **900** seconds.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to set the CDP interval frequency to 15 seconds:

```
Matrix(rw)->set cdp interval 15
```

set cdp hold-time

Use this command to set the hold time value for CDP discovery protocol configuration messages.

Syntax

set cdp hold-time *hold-time*

Parameters

hold-time	Specifies the hold time value for CDP messages in seconds.Valid values are from **15 to 600**.

Defaults

None.

Mode

Switch command, Read-Write.

Downloaded from www.Manualslib.com manuals search engine

Example

This example shows how to set CDP hold time to 60 seconds:

```
Matrix(rw)->set cdp hold-time 60
```

clear cdp

Use this command to reset CDP discovery protocol settings to defaults.

Syntax

clear cdp {[**state**] [**port-state** *port-string*] [**interval**] [**hold-time**] [**auth-code**]}

Parameters

state	(Optional) Resets the global CDP state to auto-enabled.
port-state *port-string*	(Optional) Resets the port state on specific port(s) to auto-enabled.
interval	(Optional) Resets the message frequency interval to **60** seconds.
hold-time	(Optional) Resets the hold time value to **180** seconds.
auth-code	(Optional) Resets the authentication code to 16 bytes of 00 (**00-00-00-00-00-00-00-00**).

Defaults

At least one optional parameter must be entered.

Mode

Switch command, Read-Write.

Example

This example shows how to reset the CDP state to auto-enabled:

```
Matrix(rw)->clear cdp state
```


Downloaded from www.Manualslib.com manuals search engine

Cisco Discovery Protocol

Purpose

To enable and configure the Cisco Discovery Protocol, used to discover network topology. When enabled, the Cisco Discovery Protocol allows Cisco devices to send periodic PDUs about themselves to neighboring devices. The Cisco Discovery Protocol is also used to manage the Cisco module of the Convergence End Points (CEP) IP phone detection function described in "Configuring Convergence End Points (CEP) Phone Detection" on page 25-39.

Commands

For information about...	Refer to page...
show ciscodp	3-8
show ciscodp port info	3-9
set ciscodp status	3-10
set ciscodp timer	3-11
set ciscodp holdtime	3-11
set ciscodp port	3-12
clear ciscodp	3-13

show ciscodp

Use this command to display global Cisco Discovery Protocol information.

Syntax

show ciscodp

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Only.

Example

This example shows how to display Cisco Discovery Protocol information. In this case, defaults have not been changed:

```
Matrix>show ciscodp
CiscoDP : Auto
Timer : 60
Holdtime (TTL) : 180
```


Downloaded from www.Manualslib.com manuals search engine

```
Device ID : 00E06314BD57
Last Change : WED FEB 08 01:07:45 2006
```

Table 3-2 provides an explanation of the command output.

Table 3-2 show ciscodp Output Details

Output...	What it displays...
CiscoDP	Whether Cisco Discovery Protocol is disabled or enabled globally. Auto indicates that Cisco DP will be globally enabled only if Cisco DP PDUs are received. Default setting of auto can be changed with the **set ciscodp status** command as described in "set ciscodp status" on page 3-10.
Timer	Number of seconds between Cisco Discovery Protocol PDU transmissions. Default value of **60** can be changed with the **set ciscodp timer** command as described in "set ciscodp timer" on page 3-11.
Holdtime (TTL)	Number of seconds neighboring devices will hold PDU transmissions from the sending device. Default value of **180** can be changed with the **set ciscodp holdtime** command as described in "set ciscodp holdtime" on page 3-11.
Device ID	The MAC address of the switch.
Last Change	The time that the last Cisco DP neighbor was discovered.

show ciscodp port info

Use this command to display summary information about the Cisco Discovery Protocol on one or more ports.

Syntax

show ciscodp port info [*port-string*]

Parameters

port-string	(Optional) Displays information about specific port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.

Defaults

If *port-string* is not specified, CiscoDP information will be displayed for all ports.

Mode

Switch command, Read-Only.

Example

This example shows how to display Cisco Discovery Protocol information for ports fe.1.1 through fe.1.5:

```
Matrix>(su)->show ciscodp port info fe.1.1-5
 port       state    vvid      trust      cos
-----------------------------------------------
```


Downloaded from www.Manualslib.com manuals search engine

```
fe.1.1      enabled   none      untrusted    0
fe.1.2      enabled   none      untrusted    0
fe.1.3      enabled   none      untrusted    0
fe.1.4      enabled   none      untrusted    0
fe.1.5      enabled   none      untrusted    1
```

Table 3-3 provides an explanation of the command output.

Table 3-3 show port ciscodp info Output Details

Output...	What it displays...
Port	Port designation.
State	Whether CiscoDP is enabled or disabled on this port. Default state of enabled can be changed using the **set ciscodp port** command (“set ciscodp port” on page 3-12).
VVID	Whether a Voice VLAN ID has been set on this port. Default of none can changed using the **set ciscodp port** command (“set ciscodp port” on page 3-12).
Trust	The trust mode of the port. Default of trusted can be changed using the **set ciscodp port** command (“set ciscodp port” on page 3-12).
CoS	The Class of Service priority value for untrusted traffic. The default of 0 can be changed using the **set ciscodp port** command (“set ciscodp port” on page 3-12).

set ciscodp status

Use this command to enable or disable Cisco Discovery Protocol globally on the device.

Syntax

set ciscodp status {**auto** | **enable** | **disable**}

Parameters

auto	Globally enables only if CiscoDP PDUs are received.
enable	Globally enables Cisco Discovery Protocol.
disable	Globally disables Cisco Discovery Protocol.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to enable Cisco Discovery Protocol on the device:

```
Matrix>set ciscodp status enable
```


Downloaded from www.Manualslib.com manuals search engine

set ciscodp timer

Use this command to set the number of seconds between Cisco Discovery Protocol PDU transmissions.

Syntax

set ciscodp timer *time*

Parameters

time	Specifies the number of seconds between CiscoDP PDU transmissions. Valid values are **5** - **254**.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to set the Cisco Discovery Protocol timer to 120 seconds:

```
Matrix>set ciscodp timer 120
```

set ciscodp holdtime

Use this command to set the time to live (TTL) for Cisco Discovery Protocol PDUs. This is the amount of time (in seconds) neighboring devices will hold PDU transmissions from the sending device.

Syntax

set ciscodp holdtime *time*

Parameters

time	Specifies the time to live for CiscoDP PDUs. Valid values are **10** - **255**.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to set the Cisco Discovery Protocol hold time to 180 seconds:

```
Matrix>set ciscodp holdtime 180
```


Downloaded from www.Manualslib.com manuals search engine

set ciscodp port

Use this command to set the status, voice VLAN, extended trust mode, and CoS priority for untrusted traffic for the Cisco Discovery Protocol on one or more ports.

Syntax

set ciscodp port { [**status** {**disable** | **enable**}] [**vvid** {*<vlan-id>* | **none** | **dot1p** | **untagged**}] [**trust-ext** {**trusted** | **untrusted**}] [**cos-ext** *value*] } *<port-string>*

Parameters

status	Sets the CiscoDP port operational status.
disable	Does not transmit or process CiscoDP PDUs.
enable	Transmits and processes CiscoDP PDUs.
vvid	Sets the port voice VLAN for CiscoDP PDU transmission.
<vlan-id>	Specifies the VLAN ID, range 1-4094.
none	No voice VLAN will be used in CiscoDP PDUs.
dot1p	Instructs attached phone to send 802.1p tagged frames.
untagged	Instructs attached phone to send untagged frames.
trust-ext	Sets the extended trust mode on the port.
trusted	Instructs attached phone to allow the device connected to it to transmit traffic containing any CoS or Layer 2 802.1p marking. This is the default value.
untrusted	Instructs attached phone to overwrite the 802.1p tag of traffic transmitted by the device connected to it to 0, by default, or to the value configured with the **cos-ext** parameter.
cos-ext *value*	Instructs attached phone to overwrite the 802.1p tag of traffic transmitted by the device connected to it with the specified *value*, when the trust mode of the port is set to untrusted. *Value* can range from 0 to 7, with 0 indicating the lowest priority.
port-string	Specifies the port(s) on which status will be set. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.

Defaults

None.

Mode

Switch command, Read-Write.

Usage



Note: The Cisco Discovery Protocol must be globally enabled using the **set ciscodp status** command as described in "set ciscodp status" on page 3-10 before operational status can be set on individual ports.

The following points describe how the Cisco DP extended trust settings work on the Matrix device.

Downloaded from www.Manualslib.com manuals search engine

- A Cisco DP port trust status of trusted or untrusted is only meaningful when a Cisco IP phone is connected to a switch port and a PC or other device is connected to the back of the Cisco IP phone.
- A Cisco DP port state of trusted or untrusted only affects tagged traffic transmitted by the device connected to the Cisco IP phone. Untagged traffic transmitted by the device connected to the Cisco IP phone is unaffected by this setting.
- If the switch port is configured to a Cisco DP trust state of **trusted** (with the **trust-ext trusted** parameter of this command), this setting is communicated to the Cisco IP phone instructing it to allow the device connected to it to transmit traffic containing any CoS or Layer 2 802.1p marking.
- If the switch port is configured to a Cisco DP trust state of **untrusted**, this setting is communicated to the Cisco IP phone instructing it to overwrite the 802.1p tag of traffic transmitted by the device connected to it to 0, by default, or to the value specified by the **cos-ext** parameter of this command.
- There is a one-to-one correlation between the value set with the **cos-ext** parameter and the 802.1p value assigned to ingressed traffic by the Cisco IP phone. A value of 0 equates to an 802.1p priority of 0. Therefore, a value of 7 is given the highest priority.

Examples

This example shows how to set the Cisco DP port voice VLAN ID to 3 on port fe.1.6 and enable the port operational state:

```
Matrix>set ciscodp port status enable vvid 3 fe.1.6
```

This example shows how to set the Cisco DP extended trust mode to untrusted on port fe.1.5 and set the CoS priority to 1:

```
Matrix>set ciscodp port trust-ext untrusted cos-ext 1 fe.1.5
```

clear ciscodp

Use this command to clear the Cisco Discovery Protocol back to the default values.

Syntax

clear ciscodp { [**status** | **timer** | **holdtime** | **port** {**status** | **vvid** | **trust-ext** | **cos-ext**}] } *<port-string>*

Parameters

status	Clears global CiscoDP enable status to default of auto.
timer	Clears the time between CiscoDP PDU transmissions to default of 60 seconds.
holdtime	Clears the time-to-live for CiscoDP PDU data to default of 180 seconds.
port	Clears the CiscoDP port configuration.
status	Clears the individual port operational status to the default of enabled.
vvid	Clears the individual port voice VLAN for CiscoDP PDU transmission to 0.
trust-ext	Clears the trust mode configuration of the port to trusted.

Downloaded from www.Manualslib.com manuals search engine

cos-ext	Clears the CoS priority for untrusted traffic of the port to 0.
port-string	Specifies the port(s) on which status will be set. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.

Defaults

None.

Mode

Switch command, Read-Write.

Examples

This example shows how to clear all the Cisco DP parameters back to the default settings:

```
Matrix>clear ciscodp
```

This example shows how to clear the Cisco DP port status on port fe.1.5:

```
Matrix>clear ciscodp port status fe.1.5
```


Downloaded from www.Manualslib.com manuals search engine

Link Layer Discovery Protocol and LLDP-MED

The IEEE 802.1AB standard, commonly referred to as the Link Layer Discovery Protocol (LLDP), is described in "IEEE 802.1AB-2005 Edition, IEEE Standard for Local and Metropolitan Networks: Station and Media Access Control Connectivity Discovery, May 2005."

LLDP-MED is described in the ANSI TIA Standards document "TIA-1057-2006, Link Layer Discovery Protocol for Media Endpoint Devices."

LLDP is similar to the Enterasys Discovery Protocol and the Cisco Discovery Protocol in that it provides an industry standard, vendor-neutral way to allow network devices to advertise their identities and capabilities on a local area network, and to discover that information about their neighbors.

LLDP operates on physical ports. LLDP is not supported on LAG ports.

LLDP-MED is an enhancement to LLDP that provides the following benefits:

- Auto-discovery of LAN policies, such as VLAN id, 802.1p priority, and DiffServ codepoint settings, leading to "plug-and-play" networking
- Device location and topology discovery, allowing creation of location databases and, in the case of VoIP, provision of E911 services
- Extended and automated power management of Power over Ethernet endpoints
- Inventory management, allowing network administrators to track their network devices and to determine their characteristics, such as manufacturer, software and hardware versions, and serial or asset numbers

The information sent by an LLDP-enabled device is extracted and tabulated by its peers. The communication can be done when information changes or on a periodic basis. The information tabulated is aged to ensure that it is kept up to date. Ports can be configured to send this information, receive this information, or both send and receive.

Either LLDP or LLDP-MED, but not both, can be used on an interface between two devices. A switch port uses LLDP-MED when it detects that an LLDP-MED-capable device is connected to it.

LLDP Frames

LLDP information is contained within a Link Layer Discovery Protocol Data Unit (LLDPDU) sent in a single 802.3 Ethernet frame. The information fields in LLDPDU are a sequence of short, variable-length, information elements known as TLVs — type, length, and value fields where:

- Type identifies what kind of information is being sent
- Length indicates the length of the information string in octets
- Value is the actual information that needs to be sent

The standard specifies that certain TLVs are mandatory in transmitted LLDPDUs, while others are optional. You can configure on a port-specific basis which optional LLDP and LLDP-MED TLVs should be sent in LLDPDUs.

Configuration Tasks

The commands included in this implementation allow you to perform the following configuration tasks:

Downloaded from www.Manualslib.com manuals search engine

Step	Task	Command(s)

1.	Configure global system LLDP parameters	`set lldp tx-interval`
		`set lldp hold-multiplier`
		`set lldp trap-interval`
		`set lldp med-fast-repeat`
		`clear lldp`

2.	Enable/disable specific ports to:
	• Transmit and process received LLDPDUs
	• Send LLDP traps
	• Send LLDP-MED traps
		`set/clear lldp port status`
		`set/clear lldp port trap`
		`set/clear lldp port med-trap`

3.	Configure an ECS ELIN value for specific ports	`set/clear lldp port location-info`
4.	Configure Network Policy TLVs for specific ports	`set/clear lldp port network-policy`
5.	Configure which optional TLVs should be sent by specific ports. For example, if you configured an ECS ELIN and/or Network Policy TLVs, you must enable those optional TLVs to be transmitted on the specific ports.	`set/clear lldp tx-tlv`

Commands

For information about...	Refer to page...
show lldp	3-17
show lldp port status	3-18
show lldp port trap	3-18
show lldp port tx-tlv	3-19
show lldp port location-info	3-20
show lldp port local-info	3-20
show lldp port remote-info	3-23
show lldp port network-policy	3-24
set lldp tx-interval	3-26
set lldp hold-multiplier	3-26
set lldp trap-interval	3-27
set lldp med-fast-repeat	3-27
set lldp port status	3-28
set lldp port trap	3-29
set lldp port med-trap	3-29
set lldp port location-info	3-30
set lldp port tx-tlv	3-30
set lldp port network-policy	3-32

Downloaded from www.Manualslib.com manuals search engine

For information about...	Refer to page...
clear lldp	3-34
clear lldp port status	3-34
clear lldp port trap	3-35
clear lldp port med-trap	3-35
clear lldp port location-info	3-36
clear lldp port network-policy	3-36
clear lldp port tx-tlv	3-37

show lldp

Use this command to display LLDP configuration information.

Syntax

show lldp

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Only.

Example

This example shows how to display LLDP configuration information.

```
Matrix(ro)->show lldp
Message Tx Interval        : 30
Message Tx Hold Multiplier : 4
Notification Tx Interval   : 5
MED Fast Start Count       : 3
Tx-Enabled Ports           : ge.1.1-60; ge.2.1-24; ge.3.1-30; ge.4.1-12;
                             ge.5.1-12; tg.6.1-2; fe.7.1-48
Rx-Enabled Ports           : ge.1.1-60; ge.2.1-24; ge.3.1-30; ge.4.1-12;
                             ge.5.1-12;tg.6.1-2; fe.7.1-48
Trap-Enabled Ports         : ge.1.1-60; ge.2.1-24; ge.3.1-30; ge.4.1-12;
                             ge.5.1-12; tg.6.1-2; fe.7.1-48
MED Trap-Enabled Ports     : ge.1.1-60; ge.2.1-24; ge.3.1-30; ge.4.1-12;
                             ge.5.1-12;tg.6.1-2; fe.7.1-48
```


Downloaded from www.Manualslib.com manuals search engine

show lldp port status

Use this command to display the LLDP status of one or more ports.

Syntax

show lldp port status [*port-string*]

Parameters

port-string	(Optional) Displays LLDP status for one or a range of ports.

Defaults

If *port-string* is not specified, LLDP status information will be displayed for all ports.

Mode

Switch command, Read-Only.

Usage

The command lists the ports that are enabled to send and receive LLDPPDUs. Ports are enabled or disabled with the set lldp port status command.

Example

This example shows how to display LLDP port status information for all ports.

```
Matrix(ro)->show lldp port status

Tx-Enabled Ports      : ge.1.1-60; ge.2.1-24; ge.3.1-30; ge.4.1-12; ge.5.1-12;
                        tg.6.1-2; fe.7.1-48
Rx-Enabled Ports      : ge.1.1-60; ge.2.1-24; ge.3.1-30; ge.4.1-12; ge.5.1-12;
                        tg.6.1-2; fe.7.1-48
```

show lldp port trap

Use this command to display the ports that are enabled to send an LLDP notification when a remote system change has been detected or an LLDP-MED notification when a change in the topology has been sensed.

Syntax

show lldp port trap [*port-string*]

Parameters

port-string	(Optional) Displays the port or range of ports that have been enabled to send LLDP and/or LLDP-MED notifications.

Defaults

If *port-string* is not specified, LLDP port trap information will be displayed for all ports.

Downloaded from www.Manualslib.com manuals search engine

Mode

Switch command, Read-Only.

Usage

Ports are enabled to send LLDP notifications with the set lldp port trap command and to send LLDP-MED notifications with the set lldp port med-trap command.

Example

This example shows how to display LLDP port trap information for all ports.

```
Matrix(ro)->show lldp port trap

Trap-Enabled Ports    :
MED Trap-Enabled Ports:
```

show lldp port tx-tlv

Use this command to display information about which optional TLVs have been configured to be transmitted on ports.

Syntax

show lldp port tx-tlv [*port-string*]

Parameters

port-string	(Optional) Displays information about TLV configuration for one or a range of ports.

Defaults

If *port-string* is not specified, TLV configuration information will be displayed for all ports.

Mode

Switch command, Read-Only.

Usage

Ports are configured to send optional TLVs with the set lldp port tx-tlv command.

Example

This example shows how to display transmit TLV information for three ports.

```
Matrix(ro)->show lldp port tx-tlv ge.1.1-3

* Means TLV is supported and enabled on this port
o Means TLV is supported on this port
  Means TLV is not supported on this port
Column Pro Id uses letter notation for enable: s-stp, l-lacp, g-gvrp

Ports    Port Sys  Sys  Sys Mgmt Vlan Pro  MAC PoE Link Max   MED MED MED MED
```


Downloaded from www.Manualslib.com manuals search engine

```
          Desc Name Desc Cap Addr Id   Id   PHY     Aggr Frame Cap Pol Loc PoE
-------   ---- ---- ---- --- ---- ---- ---- --- --- ---- ----  --- --- --- ---
ge.1.1    *    *    *    *   *    *    slg  *       *    *     *   *   *
ge.1.2    *    *    *    *   *    *    slg  *       *    *     *   *   *
ge.1.3    *    *    *    *   *    *    slg  *       *    *     *   *   *
```

show lldp port location-info

Use this command to display configured location information for one or more ports.

Syntax

show lldp port location-info [*port-string*]

Parameters

port-string	(Optional) Displays port location information for one or a range of ports.

Defaults

If *port-string* is not specified, port location configuration information will be displayed for all ports.

Mode

Switch command, Read-Only.

Usage

Ports are configured with a location value using the set lldp port location-info command.

Example

This example shows how to display port location information for three ports.

```
Matrix(ro)->show lldp port location-info ge.1.1-3

Ports      Type            Location
--------   -------------   -------------------------
ge.1.1     ELIN             1234567890
ge.1.2     ELIN             1234567890
ge.1.3     ELIN             1234567890
```

show lldp port local-info

Use this command to display the local system information stored for one or more ports.

Syntax

show lldp port local-info [*port-string*]

Downloaded from www.Manualslib.com manuals search engine

Parameters

port-string	(Optional) Displays local system information for one or a range of ports.

Defaults

If *port-string* is not specified, local system information will be displayed for all ports.

Mode

Switch command, Read-Only.

Usage

You can use this information to detect misconfigurations or incompatibilities between the local port and the attached endpoint device (remote port).

Example

This example shows how to display the local system information stored for port fe.4.1. Table 3-4 describes the output fields of this command.

```
Matrix(rw)->show lldp port local-info fe.4.1

Local Port  : fe.4.1      Local Port Id: fe.4.1
--------------------
Port Desc   : ... 100BASE-TX RJ21 Fast Ethernet Frontpanel Port
Mgmt Addr   : 10.21.64.100
Chassis ID  : 00-E0-63-93-74-A5
Sys Name    : LLDP PoE test Chassis
Sys Desc    : Enterasys Networks, Inc. Matrix E7 Gold Rev 05.41
Sys Cap Supported/Enabled     : bridge,router/bridge

Auto-Neg Supported/Enabled    : yes/yes
Auto-Neg Advertised           : 10BASE-T, 10BASE-TFD,
                                100BASE-TX, 100BASE-TXFD,
                                1000BASE-TFD,
                                Bpause
```

Table 3-4 describes the information displayed by the **show lldp port local-info** command.

Table 3-4 show lldp port local-info Output Details

Output...	What it displays...
Local Port	Identifies the port for which local system information is displayed.
Local Port Id	Mandatory basic LLDP TLV that identifies the port transmitting the LLDPDU. Value is ifName object defined in RFC 2863.
Port Desc	Optional basic LLDP TLV. Value is ifDescr object defined in RFC 2863.
Mgmt Addr	Optional basic LLDP TLV. IPv4 address of host interface.
Chassis ID	Mandatory basic LLDP TLV that identifies the chassis transmitting the LLDPDU. Value is MAC address of chassis.

Downloaded from www.Manualslib.com manuals search engine

Table 3-4 show lldp port local-info Output Details (continued)

Output...	What it displays...
Sys Name	Optional basic LLDP TLV. Value is the administratively assigned name for the system.
Sys Desc	Optional basic LLDP TLV. Value is sysDescr object defined in RFC 3418.
Sys Cap Supported/Enabled	Optional basic LLDP TLV. System capabilities, value can be bridge and/or router.
Auto-Neg Supported/Enabled	IEEE 802.3 Extensions MAC-PHY Configuration/Status TLV. Auto-negotiation supported and enabled settings should be the same on the two systems attached to the same link.
Auto-Neg Advertised	IEEE 802.3 Extensions MAC-PHY Configuration/Status TLV. Lists the configured advertised values on the port.
Operational Speed/Duplex/Type	IEEE 802.3 Extensions MAC-PHY Configuration/Status TLV. Lists the operational MAU type, duplex, and speed of the port. If the received TLV indicates that auto-negotiation is supported but not enabled, these values will be used by the port.
Max Frame Size (bytes)	IEEE 802.3 Extensions Maximum Frame Size TLV. Value indicates maximum frame size capability of the device's MAC and PHY. In normal mode, max frame size is 1522 bytes. In jumbo mode, max frame size is 10239 bytes.
Vlan Id	IEEE 802.1 Extensions Port VLAN ID TLV. Value is port VLAN ID (pvid).
LAG Supported/Enabled/Id	IEEE 802.3 Extensions Link Aggregation TLV. Values indicate whether the link associated with this port can be aggregated, whether it is currently aggregated, and if aggregated, the aggregated port identifier.
Protocol Id	IEEE 802.1 Extensions Protocol Identity TLV. Values can include Spanning tree, LACP, and GARP protocols and versions. Only those protocols enabled on the port are displayed.
Network Policy (app/tag/vlanId/cos/dscp)	LLDP-MED Extensions Network Policy TLV. For all applications enabled on the port to be transmitted in a TLV, displays the application name, VLAN type (tagged or untagged), VLAN Id, and both the Layer 2 and Layer 3 priorities assiciated with the application.
ECS ELIN	LLDP-MED Extensions Location Identification TLV. Emergency Call Services (ECS) Emergency Location Identification Number (ELIN) is currently the only type supported. Value is the ELIN configured on this port.
PoE Device	LLDP-MED Extensions Extended Power via MDI TLV. Displayed only when a port has PoE capabilities. Value is the Power Type of the device. On a Matrix switch port, the value is Power Sourcing Entity (PSE).
PoE Power Source	LLDP-MED Extensions Extended Power via MDI TLV. Displayed only when a port has PoE capabilities. Value can be primary or backup, indicating whether the PSE is using its primary or backup power source.
PoE MDI Supported/Enabled	IEEE 802.3 Extensions Power via MDI TLV. Displayed only when a port has PoE capabilities. Indicates whether sending the Power via MDI TLV is supported/enabled. Value can be yes or no.

Downloaded from www.Manualslib.com manuals search engine

Table 3-4 show lldp port local-info Output Details (continued)

Output...	What it displays...
PoE Pair Controllable/Used	IEEE 802.3 Extensions Power via MDI TLV. Displayed only when a port has PoE capabilities. Indicates whether pair selection can be controlled on the given port (refer to RFC 3621). Value for Controllable can be true or false. Value of Used can be signal (signal pairs only are in use) or spare (spare pairs only are in use).
PoE Power Class	IEEE 802.3 Extensions Power via MDI TLV. Displayed only when a port has PoE capabilities. Indicates the power class supplied by the port. Value can range from 0 to 4.
PoE Power Limit (mW)	LLDP-MED Extensions Extended Power via MDI TLV. Displayed only when a port has PoE capabilities. Indicates the total power the port is capable of sourcing over a maximum length cable, based on its current configuration, in milli-Watts.
PoE Power Priority	LLDP-MED Extensions Extended Power via MDI TLV. Displayed only when a port has PoE capabilities. Indicates the power priority configured on the port. Value can be critical, high, or low.

show lldp port remote-info

Use this command to display the remote system information stored for a remote device connected to a local port.

Syntax

show lldp port remote-info [*port-string*]

Parameters

port-string	(Optional) Displays remote system information for one or a range of ports.

Defaults

If *port-string* is not specified, remote system information will be displayed for all ports.

Mode

Switch command, Read-Only.

Usage

You can use this information to detect misconfigurations or incompatibilities between the local port and the attached endpoint device (remote port).

Example

This example shows how to display the remote system information stored for port ge.3.1. The remote system information was received from an IP phone, which is an LLDP-MED-enabled device. Table 3-5 describes the output fields that are unique to the remote system information displayed for a MED-enabled device.

```
Matrix(ro)->show lldp port remote-info ge.3.1
Local Port  : ge.3.1     Remote Port Id : 00-09-6e-0e-14-3d
--------------------
```


Downloaded from www.Manualslib.com manuals search engine

```
Mgmt Addr    : 0.0.0.0
Chassis ID   : 0.0.0.0
Device Type : Communication Device Endpoint (class III)
Sys Name     : AVE0E143D
Sys Cap Supported/Enabled     : bridge,telephone/bridge

Auto-Neg Supported/Enabled    : yes/yes
Auto-Neg Advertised           : 10BASE-T, 10BASE-TFD
                              : 100BASE-TX, 100BASE-TXFD
                              : pause, Spause
Operational Speed/Duplex/Type : 100/full/TX
```

Note that the information fields displayed by the **show lldp port remote-info** command will vary, depending on the type of remote device that is connected to the port.

Table 3-5 describes the output fields that are unique to the remote system information database. Refer to Table 3-4 on page 21 for descriptions of the information fields that are common to both the local and the remote system information databases.

Table 3-5 show lldp port remote-info Output Display

Output...	What it displays...
Remote Port Id	Displays whatever port Id information received in the LLDPDU from the remote device. In this case, the port Id is MAC address of remote device.
Device Type	Mandatory LLDP-MED Capabilities TLV. Displayed only when the port is connected to an LLDP-MED-capable endpoint device.
Hardware Revision	LLDP-MED Extensions Inventory Management TLV component.
Firmware Revision	LLDP-MED Extensions Inventory Management TLV component.
Sofware Revision	LLDP-MED Extensions Inventory Management TLV component.
Serial Number	LLDP-MED Extensions Inventory Management TLV component.
Manufacturer	LLDP-MED Extensions Inventory Management TLV component.
Model Number	LLDP-MED Extensions Inventory Management TLV component.
Asset ID	LLDP-MED Extensions Inventory Management TLV component. In the above example, no asset ID was received from the remote device so the field is not displayed.

show lldp port network-policy

Use this command to display LLDP port network policy configuration information. Network policy information is configured using the set lldp port network-policy command.

Syntax

show lldp port network policy {**all** | **voice** | **voice-signaling** | **guest-voice** | **guest-voice-signaling** | **software-voice** | **video-conferencing** | **streaming-video** | **video-signaling** } [*port-string*]

Downloaded from www.Manualslib.com manuals search engine

Parameters

all	Displays information about all network policy applications.
voice	Displays information about only the voice application type.
voice-signaling	Displays information about only the voice signaling application type.
guest-voice	Displays information about only the guest voice application type.
guest-voice-signaling	Displays information about only the guest voice signaling application type.
software-voice	Displays information about only the softphone voice application type.
video-conferencing	Displays information about only the video conferencing application type.
streaming-video	Displays information about only the streaming video application type.
video-signaling	Displays information about only the video signaling application type.
port-string	(Optional) Displays information about LLDP network policy for one or a range of ports.

Defaults

If *port-string* is not specified, only non-default values will be displayed for all ports that have non-default values configured.

If a *port-string* is specified, then all values, default and non-default, are displayed for the specified ports.

Mode

Switch command, Read-Only.

Example

This example shows how to display all LLDP network policy information for ge.1.1.

```
Matrix(ro)->show lldp port network-policy all ge.1.1

Ports    Application            State     Tag       Vlan-Id   Cos   Dscp
-------  ---------------------  --------  --------  -------   ---   ---
ge.1.1   voice                  enabled   untagged  1         0     0
         voice signaling        enabled   untagged  1         0     0
         guest voice            enabled   untagged  1         0     0
         guest voice signaling  enabled   untagged  1         0     0
         softphone voice        enabled   untagged  1         0     0
         video conferencing     enabled   untagged  1         0     0
         streaming video        enabled   untagged  1         0     0
         video signaling        enabled   untagged  1         0     0
```


Downloaded from www.Manualslib.com manuals search engine

set lldp tx-interval

Use this command to set the time, in seconds, between successive LLDP frame transmissions initiated by changes in the LLDP local system information.

Syntax

set lldp tx-interval *frequency*

Parameters

frequency	Specifies the number of seconds between transmissions of LLDP frames. Value can range from 5 to 32,768 seconds. The default is 30 seconds.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example sets the transmit interval to 20 seconds.

```
Matrix(rw)->set lldp tx-interval 20
```

set lldp hold-multiplier

Use this command to set the time-to-live value used in LLDP frames sent by this device.

Syntax

set lldp hold-multiplier *multiplier-val*

Parameters

multiplier-val	Specifies the multiplier to apply to the transmit interval to determine the time-to-live value. Value can range from 2 to 10. Default value is 4.

Defaults

None.

Mode

Switch command, Read-Write.

Usage

The time-to-live for LLDPDU data is calculated by multiplying the transmit interval by the hold multiplier value.

Downloaded from www.Manualslib.com manuals search engine

Example

This example sets the transmit interval to 20 seconds and the hold multiplier to 5, which will configure a time-to-live of 100 to be used in the TTL field in the LLDPDU header.

```
Matrix(rw)->set lldp tx-interval 20
Matrix(rw)->set lldp hold-multiplier 5
```

set lldp trap-interval

Use this command to set the minimum interval between LLDP notifications sent by this device. LLDP notifications are sent when a remote system change has been detected.

Syntax

set lldp trap-interval *frequency*

Parameters

frequency	Specifies the minimum time between LLDP trap transmissions, in seconds. The value can range from 5 to 3600 seconds. The default value is 5 seconds.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example sets the minimum interval between LLDP traps to 10 seconds.

```
Matrix(rw)->set lldp trap-interval 10
```

set lldp med-fast-repeat

Network connectivity devices transmit only LLDP TLVs in LLDPDUs until they detect that an LLDP-MED endpoint device has connected to a port.

Syntax

set lldp med-fast-repeat *count*

Parameters

count	Specifies the number of fast start LLDPDUs to be sent when an LLDP-MED endpoint device is detected. Value can range from 1 to 10. Default is 3.

Defaults

None.

Downloaded from www.Manualslib.com manuals search engine

Mode

Switch command, Read-Write.

Usage

When an LLDP-MED endpoint device has connected to a port, the network connectivity device starts sending LLDP-MED TLVs at a fast start rate on that port. Use this command to set the number of successive LLDPDUs (with LLDP-MED TLVs) to be sent for one complete fast start interval.

Example

This example sets the number of fast start LLDPDUs to be sent to 4.

```
Matrix(rw)->set lldp med-fast-repeat 4
```

set lldp port status

Use this command to enable or disable transmitting and processing received LLDPDUs on a port or range of ports.

Syntax

set lldp port status {**tx-enable** | **rx-enable** | **both** | **disable**} *port-string*

Parameters

tx-enable	Enables transmitting LLDPDUs on the specified ports.
rx-enable	Enables receiving and processing LLDPDUs from remote systems on the specified ports.
both	Enables both transmitting and processing received LLDPDUs on the specified ports.
disable	Disables both transmitting and processing received LLDPDUs on the specified ports.
port-string	Specifies the port or range of ports to be affected.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example enables both transmitting LLDPDUs and receiving and processing LLDPDUs from remote systems on ports ge.1.1 through ge.1.6.

```
Matrix(rw)->set lldp port status both ge.1.1-6
```


Downloaded from www.Manualslib.com manuals search engine

set lldp port trap

Use this command to enable or disable sending LLDP notifications (traps) when a remote system change is detected.

Syntax

set lldp port trap {**enable** | **disable**} *port-string*

Parameters

enable	Enables transmitting LLDP traps on the specified ports.
disable	Disables transmitting LLDP traps on the specified ports.
port-string	Specifies the port or range of ports to be affected.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example enables transmitting LLDP traps on ports ge.1.1 through ge.1.6.

```
Matrix(rw)->set lldp port trap enable ge.1.1-6
```

set lldp port med-trap

Use this command to enable or disable sending an LLDP-MED notification when a change in the topology has been sensed on the port (that is, a remote endpoint device has been attached or removed from the port).

Syntax

set lldp port med-trap {**enable** | **disable**} *port-string*

Parameters

enable	Enable transmitting LLDP-MED traps on the specified ports.
disable	Disable transmitting LLDP-MED traps on the specified ports.
port-string	Specifies the port or range of ports to be affected.

Defaults

None.

Mode

Switch command, Read-Write.

Downloaded from www.Manualslib.com manuals search engine

Example

This example enables transmitting LLDP-MED traps on ports ge.1.1 through ge.1.6.

```
Matrix(rw)->set lldp port med-trap enable ge.1.1-6
```

set lldp port location-info

Use this command to configure LLDP-MED location information on a port or range of ports. Currently, only Emergency Call Services (ECS) Emergency Location Identification Number (ELIN) is supported.

Syntax

set lldp port location-info elin *elin-string port-string*

Parameters

elin	Specifies that the ECS ELIN data format is to be used.
elin-string	Specifies the location identifier. Value can be from 10 to 25 numerical characters.
port-string	Specifies the port or range of ports to be affected.

Defaults

None.

Mode

Switch command, Read-Write.

Example

After you configure a location information value, you must also configure the port to send the Location Information TLV with the set lldp port tx-tlv command. This example configures the ELIN identifier 5551234567 on ports ge.1.1 through ge.1.6 and then configures the ports to send the Location Information TLV.

```
Matrix(rw)->set lldp port location-info 5551234567 ge.1.1-6
Matrix(rw)->set lldp port tx-tlv med-loc ge.1.1-6
```

set lldp port tx-tlv

Use this command to select the optional LLDP and LLDP-MED TLVs to be transmitted in LLDPDUs by the specified port or ports. Use the show lldp port local-info command to display the values of these TLVs for the port.

Syntax

set lldp port tx-tlv {[**all**] | [**port-desc**] [**sys-name**] [**sys-desc**] [**sys-cap**] [**mgmt-addr**] [**vlan-id**] [**stp**] [**lacp**] [**gvrp**] [**mac-phy**] [**poe**] [**link-aggr**] [**max-frame**] [**med-cap**] [**med-pol**] [**med-loc**] [**med-poe**]} *port-string*

Downloaded from www.Manualslib.com manuals search engine

Parameters

all	Add all optional TLVs to transmitted LLDPDUs.
port-desc	Port Description optional basic LLDP TLV. Value sent is ifDescr object defined in RFC 2863.
sys-name	System Name optional basic LLDP TLV. Value sent is the administratively assigned name for the system.
sys-desc	System Description optional basic LLDP TLV. Value sent is sysDescr object defined in RFC 3418.
sys-cap	System Capabilities optional basic LLDP TLV. For a network connectivity device, value sent can be bridge and/or router.
mgmt-addr	Management Address optional basic LLDP TLV. Value sent is IPv4 address of host interface.
vlan-id	Port VLAN ID IEEE 802.1 Extensions TLV. Value sent is port VLAN ID (PVID).
stp	Spanning Tree information defined by Protocol Identity IEEE 802.1 Extensions TLV. If STP is enabled on the port, value sent includes version of protocol being used.
lacp	LACP information defined by Protocol Identity IEEE 802.1 Extensions TLV. If LACP is enabled on the port, value sent includes version of protocol being used.
gvrp	GVRP information defined by Protocol Identity IEEE 802.1 Extensions TLV. If LACP is enabled on the port, value sent includes version of protocol being used.
mac-phy	MAC-PHY Configuration/Status IEEE 802.3 Extensions TLV. Value sent includes the operational MAU type, duplex, and speed of the port.
poe	Power via MDI IEEE 802.3 Extensions TLV. Values sent include whether pair selection can be controlled on port, and the power class supplied by the port. Only valid for PoE-enabled ports.
link-aggr	Link Aggregation IEEE 802.3 Extensions TLV. Values sent indicate whether the link associated with this port can be aggregated, whether it is currently aggregated, and if aggregated, the aggregated port identifier.
max-frame	Maximum Frame Size IEEE 802.3 Extensions TLV. Value sent indicates maximum frame size of the port's MAC and PHY.
med-cap	LLDP-MED Capabilities TLV.Value sent indicates the capabilities (whether the device supports location information, network policy, extended power via MDI) and Device Type (network connectivity device) of the sending device.
med-pol	LLDP-MED Network Policy TLV. Values sent include application name, VLAN type (tagged or untagged), VLAN ID, and both Layer 2 and Layer 3 priorities associated with application, for all applications enabled on the port. See the set lldp port network-policy command for more information.
med-loc	LLDP-MED Location Identification TLV. Value sent is the ECS ELIN value configured on the port. See the set lldp port location-info command for more information.

Downloaded from www.Manualslib.com manuals search engine

med-poe	LLDP-MED Extended Power via MDI TLV. Values sent include the Power Limit (total power the port is capable of sourcing over a maximum length cable) and the power priority configured on the port. Only valid for PoE-enabled ports.
port-string	Specifies the port or range of ports to be affected.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example configures the management address, MED capability, MED network policy, and MED location identification TLVs to be sent in LLDPDUs by port ge.1.1.

```
Matrix(rw)->set lldp port tx-tlv mgmt-addr med-cap med-pol med-loc ge.1.1
```

set lldp port network-policy

Use this command to configure network policy for a set of applications on a port or range of ports.

Syntax

set lldp port network-policy {**all** | **voice** | **voice-signaling** | **guest-voice** | **guest-voice-signaling** | **softphone-voice** | **video-conferencing** | **streaming-video** | **video-signaling**} [**state** {**enable** | **disable**}] [**tag** {**tagged** | **untagged**}] [**vid** {*vlan-id* | **dot1p**}] [**cos** *cos-value*] [**dscp** *dscp-value*] *port-string*

Parameters

all	Configures all applications.
voice	Configures the voice application.
voice-signaling	Configures the voice signaling application. This application will not be advertised if the **voice** application is configured with the same parameters.
guest-voice	Configures the guest voice application.
guest-voice-signaling	Configures the guest voice signaling application. This application will not be advertised if the **guest-voice** application is configured with the same parameters.
softphone-voice	Configures the softphone voice application.
video-conferencing	Configures the video conferencing application.
streaming-video	Configures the streaming video application.
video-signaling	Configures the video signaling application. This application will not be advertised if the **video-conferencing** application is configured with the same parameters.

Downloaded from www.Manualslib.com manuals search engine

state enable | **disable**	(Optional) Enables or disables advertising the application information being configured.
tag tagged | **untagged**	(Optional) Indicates whether the application being configured is using a tagged or untagged VLAN. If untagged, both the VLAN ID and the CoS priority fields are ignored and only the DSCP value has relevance.
vid *vlan-id* | **dot1p**	(Optional) VLAN identifier for the port. The value of *vlan-id* can range from 1 to 4094. Use **dot1p** if the device is using priority tagged frames, meaning that only the IEEE 802.1D priority level is significant and the default PVID of the ingress port is used.
cos *cos-value*	(Optional) Specifies the Layer 2 priority to be used for the application being configured. The value can range from 0 to 7. A value of 0 represents use of the default priority as defined in IEEE 802.1D.
dscp *dscp-value*	(Optional) Specifies the DSCP value to be used to provide Diffserv node behavior for the application being configured. The value can range from 0 to 63. A value of 0 represents use of the default DSCP value as defined in RFC 2475.
port-string	Specifies the port or range of ports to be affected.

Defaults

None.

Mode

Switch command, Read-Write.

Usage

As described in the ANSI/TIA Standards document 1057, the Network Policy TLV is "intended for use with applications that have specific real-time network policy requirements, such as interactive voice and/or video services" and should be implemented only on direct links between network connectivity devices and endpoint devices. Refer to the ANSI/TIA Standards document 1057 for descriptions of the application types.

After you configure Network Policy TLVs, you must also configure the port to send the Network Policy TLV with the set lldp port tx-tlv command.

The policies configured with this command are sent in LLDPDUs as LLDP-MED Network Policy TLVs. Multiple Network Policy TLVs can be sent in a single LLDPDU.

Example

This example configures the voice application TLV on port fe.2.1 and then configures the port to send the Network Policy TLV.

```
Matrix(rw)->set lldp port network-policy voice state enable tag tagged vlan dot1p
fe.2.1
Matrix(rw)->set lldp port tx-tlv med-pol fe.2.1
```


Downloaded from www.Manualslib.com manuals search engine

clear lldp

Use this command to return LLDP parameters to their default values.

Syntax

clear lldp {**all** | **tx-interval** | **hold-multipler** | **trap-interval** | **med-fast-repeat**}

Parameters

all	Returns **all** LLDP configuration parameters to their default values, including port LLDP configuration parameters.
tx-interval	Returns the number of seconds between transmissions of LLDP frames.to the default of 30 seconds.
hold-multiplier	Returns the multiplier to apply to the transmit interval to determine the time-to-live value to the default value of 4.
trap-interval	Returns the minimum time between LLSP trap transmissions to the default value of 5 seconds.
med-fast-repeat	Returns the number of fast start LLDPDUs to be sent when an LLDP-MED endpoint device is detected to the default of 3.

Defaults

None.

Mode

Switch command, Read-Write.

Examples

This example returns the transmit interval to the default value of 30 seconds.

```
Matrix(rw)->clear lldp tx-interval
```

clear lldp port status

Use this command to return the port status to the default value of both (both transmitting and processing received LLDPDUs are enabled).

Syntax

clear lldp port status *port-string*

Parameters

port-string	Specifies the port or range of ports to be affected.

Defaults

None.

Mode

Switch command, Read-write.

Downloaded from www.Manualslib.com manuals search engine

Example

This example returns port ge.1.1 to the default state of enabled for both transmitting and processing received LLDPDUs.

```
Matrix(rw)->clear lldp port status ge.1.1
```

clear lldp port trap

Use this command to return the port LLDP trap setting to the default value of disabled.

Syntax

clear lldp port trap *port-string*

Parameters

port-string	Specifies the port or range of ports to be affected.

Defaults

None.

Mode

Switch command, Read-write.

Example

This example returns port ge.1.1 to the default LLDP trap state of disabled.

```
Matrix(rw)->clear lldp port trap ge.1.1
```

clear lldp port med-trap

Use this command to return the port LLDP-MED trap setting to the default value of disabled.

Syntax

clear lldp port med-trap *port-string*

Parameters

port-string	Specifies the port or range of ports to be affected.

Defaults

None.

Mode

Switch command, Read-write.

Example

This example returns port ge.1.1 to the default LLDP-MED trap state of disabled.

```
Matrix(rw)->clear lldp port med-trap ge.1.1
```


Downloaded from www.Manualslib.com manuals search engine

clear lldp port location-info

Use this command to return the port ECS ELIN location setting to the default value of null.

Syntax

clear lldp port location-info elin *port-string*

Parameters

elin	Specifies that the ECS ELIN location information value should be cleared.
port-string	Specifies the port or range of ports to be affected.

Defaults

None.

Mode

Switch command, Read-write.

Example

This example returns the location information ELIN value on port ge.1.1 to the default value of null.

```
Matrix(rw)->clear lldp port location-info elin ge.1.1
```

clear lldp port network-policy

Use this command to return network policy for a set of applications on a port or range of ports to default values.

Syntax

clear lldp port network-policy {**all** | **voice** | **voice-signaling** | **guest-voice** | **guest-voice-signaling** | **softphone-voice** | **video-conferencing** | **streaming-video** | **video-signaling**} {[**state**] [**tag**] [**vid**] [**cos**] [**dscp**] } *port-string*

Parameters

all	Command will be applied to all applications.
voice	Command will be applied to the voice application.
voice-signaling	Command will be applied to the voice signaling application.
guest-voice	Command will be applied to the guest voice application.
guest-voice-signaling	Command will be applied to the guest voice signaling application.
softphone-voice	Command will be applied to the softphone voice application.
video-conferencing	Command will be applied to the video conferencing application.
streaming-video	Command will be applied to the streaming video application.
video-signaling	Command will be applied to the video signaling application.
state	(Optional) Clear the state of advertising the application information being configured to disabled.

Downloaded from www.Manualslib.com manuals search engine

tag	(Optional) Clear the tag value of the application being configured to untagged.
vid	(Optional) Clear the VLAN identifier for the port to the default value of 1.
cos	(Optional) Clear the Layer 2 priority to be used for the application being configured to the default value of 0. (A value of 0 represents use of the default priority as defined in IEEE 802.1D.)
dscp	(Optional) Clear the DSCP value to be used to provide Diffserv node behavior for the application being configured to the default value of 0. (A value of 0 represents use of the default DSCP value as defined in RFC 2475.)
port-string	Specifies the port or range of ports to be affected.

Defaults

At least one application (or **all**) and one policy parameter must be specified.

Mode

Switch command, Read-Write.

Example

This example returns all network policy values for all applications on port ge.1.1 to their default values.

```
Matrix(rw)->clear lldp port network-policy all state tag vid cos dscp ge.1.1
```

clear lldp port tx-tlv

Use this command to clear the optional LLDP and LLDP-MED TLVs to be transmitted in LLDPDUs by the specified port or ports to the default value of disabled.

Syntax

clear lldp port tx-tlv {[**all**] | [**port-desc**] [**sys-name**] [**sys-desc**] [**sys-cap**] [**mgmt-addr**] [**vlan-id**] [**stp**] [**lacp**] [**gvrp**] [**mac-phy**] [**poe**] [**link-aggr**] [**max-frame**] [**med-cap**] [**med-pol**] [**med-loc**] [**med-poe**]} *port-string*

Parameters

all	Disables all optional TLVs from being transmitted in LLDPDUs.
port-desc	Disables the Port Description optional basic LLDP TLV from being transmitted in LLDPDUs.
sys-name	Disables the System Name optional basic LLDP TLV from being transmitted in LLDPDUs.
sys-desc	Disables the System Description optional basic LLDP TLV from being transmitted in LLDPDUs.
sys-cap	Disables the System Capabilities optional basic LLDP TLV from being transmitted in LLDPDUs.
mgmt-addr	Disables the Management Address optional basic LLDP TLV from being transmitted in LLDPDUs.

Downloaded from www.Manualslib.com manuals search engine

vlan-id	Disables the Port VLAN ID IEEE 802.1 Extensions TLV from being transmitted in LLDPDUs.
stp	Disables the Spanning Tree information defined by Protocol Identity IEEE 802.1 Extensions TLV from being transmitted in LLDPDUs.
lacp	Disables the LACP information defined by Protocol Identity IEEE 802.1 Extensions TLV from being transmitted in LLDPDUs.
gvrp	Disables the GVRP information defined by Protocol Identity IEEE 802.1 Extensions TLV from being transmitted in LLDPDUs.
mac-phy	Disables the MAC-PHY Configuration/Status IEEE 802.3 Extensions TLV from being transmitted in LLDPDUs.
poe	Disables the Power via MDI IEEE 802.3 Extensions TLV from being transmitted in LLDPDUs. Only valid for PoE-enabled ports.
link-aggr	Disables the Link Aggregation IEEE 802.3 Extensions TLV from being transmitted in LLDPDUs.
max-frame	Disables the Maximum Frame Size IEEE 802.3 Extensions TLV from being transmitted in LLDPDUs.
med-cap	Disables the LLDP-MED Capabilities TLV from being transmitted in LLDPDUs.
med-pol	Disables the LLDP-MED Network Policy TLV from being transmitted in LLDPDUs.
med-loc	Disables the LLDP-MED Location Identification TLV from being transmitted in LLDPDUs.
med-poe	Disables the LLDP-MED Extended Power via MDI TLV from being transmitted in LLDPDUs. Only valid for PoE-enabled ports.
port-string	Specifies the port or range of ports to be affected.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example disables the management address, MED capability, MED network policy, and MED location identification TLVs from being sent in LLDPDUs by port ge.1.1.

```
Matrix(rw)->clear lldp port tx-tlv mgmt-addr med-cap med-pol med-loc ge.1.1
```


Downloaded from www.Manualslib.com manuals search engine

4

Port Configuration

This chapter describes the Port Configuration set of commands and how to use them.

Important Notice

CLI examples in this guide illustrate a generic Matrix command prompt and chassis-based / modular port designations. Depending on which Matrix Series device you are using, your default command prompt and output may be different than the examples shown.

For information about...	Refer to page...
Port Configuration Summary	4-1
Setting Console Port Properties	4-3
Reviewing Port Status	4-13
Disabling / Enabling and Naming Ports	4-20
Setting Speed and Duplex Mode	4-24
Enabling / Disabling Jumbo Frame Support	4-27
Setting Auto-Negotiation and Advertised Ability	4-30
Setting Flow Control	4-37
Configuring Link Traps and Link Flap Detection	4-39
Configuring Broadcast Suppression	4-49
Configuring Port Mirroring	4-52
Configuring LACP	4-55

Port Configuration Summary

Console Port(s)

Each Matrix Series module or standalone device includes a console port through which local management of the device can be accessed using a terminal or modem.

For details on configuring one or more console port settings, refer to "Setting Console Port Properties" on page 4-3.

For module placement rules and considerations for configuring local management on DFE-Gold modules, refer to the *Matrix DFE-Gold Series Installation Guide*.

For details on activating redundancy on a DFE-Gold Series module, refer to "Activating Licensed Features" on page 2-58.

Downloaded from www.Manualslib.com manuals search engine

Switch Ports

The Matrix Series modules and standalone devices have fixed front panel switch ports and, depending on the model, optional expansion module slots. The numbering scheme used to identify the switch ports on the front panel and the expansion module(s) installed is interface-type dependent and is also dependent upon the chassis in which the module(s) are installed.

Port String Syntax Used in the CLI

Commands requiring a *port-string* parameter use the following syntax to designate port type, slot location, and port number:

port type.slot location.port number

Where **port type** can be:

fe for 100-Mbps Ethernet
ge for 1-Gbps Ethernet
tg for 10-Gbps Ethernet
com for COM (console) port
host for the host port
vlan for vlan interfaces
lag for IEEE802.3 link aggregation ports
lpbk for loopback interfaces, or
lo for the local (software loopback) interface
bp for FTM1 backplane ports
pc for the internal ports which connect to the on-board processor of an installed Matrix Security Module

rtr for router interface

Slot location for modules installed in a Matrix N7 or E7 chassis can be:
0 through **7**, with **0** designating virtual system ports (lag, vlan, host, loopback), and **1** designating the left-most module slot in the chassis.

Slot location for modules installed in a Matrix N3 or N5 chassis can be:
0 through **3** or **0** through **5**, with **0** designating virtual system ports (lag, vlan, host, loopback), and **1** designating the lowest module slot in the chassis.

Port number can be:
Any port number in a slot location. The highest valid port number is dependent on the number of ports in a slot location and the port type.

For example:
If a module in slot 1 has 48, 100Mbps Fast Ethernet front panel ports, and an uplink interface with 6 Mini GBICs, the range of port number designations used in the CLI command would be:

fe.1.1 through **fe.1.48** for the 48 100Mbps Fast Ethernet front panel ports, and
ge.1.1 through **ge.1.6** for the 6 Mini GBIC uplink ports.

If the uplink has the same type (**fe**) ports as the front panel, the numbering continues with the port number **fe.1.49**.

Examples



Note: You can use a wildcard (*) to indicate all of an item. For example, fe.3.* would represent all 100Mbps Ethernet (fe) ports in the module in slot 3.

This example shows the *port-string* syntax for specifying the 100-Mbps Ethernet ports 1 through 10 in the module in chassis slot 1.

Downloaded from www.Manualslib.com manuals search engine

```
fe.1.1-10
```

This example shows the *port-string* syntax for specifying the 1-Gigabit Ethernet port 14 in the module in chassis slot 3.

```
ge.3.14
```

This example shows the *port-string* syntax for specifying Fast Ethernet ports 1 and 3 and Gigabit Ethernet port 11 in the module in chassis slot 1:

```
fe.1.1,fe.1.3;ge.1.11
```

This example shows the *port-string* syntax for specifying Fast Ethernet ports 1, 3, 7, 8, 9 and 10 in the module in chassis slot 1:

```
fe.1.1,fe.1.3,fe.1.7-10
```

This example shows the *port-string* syntax for specifying the 10-Gigabit Ethernet port 2 of the module in chassis slot 3.

```
tg.3.1
```

This example shows the *port-string* syntax for specifying all 1-Gigabit Ethernet ports in the module in chassis slot 3.

```
ge.3.*
```

This example shows the *port-string* syntax for specifying all 10-Gbps Ethernet ports in the chassis.

```
tg.*.*
```

This example shows the *port-string* syntax for specifying all ports (of any interface type) in all modules in the chassis `*.*.*`

Setting Console Port Properties

Purpose

To review and set parameters for one or more of the device's console ports, including baud rate, auto baud detection, stopbits and parity.

Commands

The commands used to review and configure console port settings are listed below and described in the associated section as shown.

For information about...	Refer to page...
show console	4-4
clear console	4-4
show console baud	4-5
set console baud	4-5
clear console baud	4-6
show console flowcontrol	4-6
set console flowcontrol	4-7
clear console flowcontrol	4-7

Downloaded from www.Manualslib.com manuals search engine

For information about...	Refer to page...
show console bits	4-8
set console bits	4-8
clear console bits	4-9
show console stopbits	4-9
set console stopbits	4-10
clear console stopbits	4-10
show console parity	4-11
set console parity	4-11
clear console parity	4-12

show console

Use this command to display properties set for one or more console ports.

Syntax

show console [*port-string*]

Parameters

port-string	(Optional) Displays properties for specific console port(s)

Defaults

If *port-string* is not specified, properties for all console ports will be displayed.

Mode

Switch command, Read-Only.

Example

This example shows how to display properties for console port com.1.1:

```
Matrix(rw)->show console com.1.1

Port          Baud    Flow    Bits  StopBits    Parity  Autobaud
------------  ------  ------  ----  ----------  ------  --------
com.1.1       38400   ctsrts  8     one         none    disable
```

clear console

Use this command to clear the properties set for one or more console ports.

Syntax

clear console [*port-string*]

Downloaded from www.Manualslib.com manuals search engine

Parameters

port-string	(Optional) Clears properties for specific console port(s).

Defaults

If *port-string* is not specified, properties for all console ports will be cleared.

Mode

Switch command, Read-Only.

Example

This example shows how to clear properties for console port com.1.1:

```
Matrix(rw)->clear console com.1.1
```

show console baud

Use this command to display the baud rate for one or more console ports.

Syntax

show console baud [*port-string*]

Parameters

port-string	(Optional) Displays baud rate for specific console port(s).

Defaults

If *port-string* is not specified, baud rate for all console ports will be displayed.

Mode

Switch command, Read-Only.

Example

This example shows how to display the baud rate for console port com.1.1:

```
Matrix(rw)->show console baud com.1.1

Port          Baud
------------  --------
com.1.1       38400
```

set console baud

Use this command to set the baud rate for one or more console ports.

Syntax

set console baud *rate* [*port-string*]

Downloaded from www.Manualslib.com manuals search engine

Parameters

rate	Sets the console baud rate. Valid values are: **300, 600**, **1200**, **2400**, **4800**, **5760**, **9600**, **14400**, **19200**, **38400**, and **115200**.
port-string	(Optional) Sets baud rate for specific port(s).

Defaults

If *port-string* is not specified, baud rate will be set for all console ports.

Mode

Switch command, Read-Write.

Example

This example shows how to set the baud rate to 19200 on console port com.1.1:

```
Matrix(rw)->set console baud 19200 com.1.1
```

clear console baud

Use this command to clear the baud rate for one or more console ports.

Syntax

clear console baud [*port-string*]

Parameters

port-string	(Optional) Clears baud rate for specific port(s).

Defaults

If *port-string* is not specified, baud rate will be cleared for all console ports.

Mode

Switch command, Read-Write.

Example

This example shows how to clear the baud rate on console port com.1.1:

```
Matrix(rw)->clear console baud com.1.1
```

show console flowcontrol

Use this command to display the type of flow control setting for one or more console ports.

Syntax

show console flowcontrol [*port-string*]

Parameters

port-string	(Optional) Displays the flow control setting for specific console port(s).

Downloaded from www.Manualslib.com manuals search engine

Defaults

If *port-string* is not specified, the flow control setting for all console ports will be displayed.

Mode

Switch command, Read-Only.

Example

This example shows how to display the flow control setting for console port com.1.1:

```
Matrix(rw)->show console flowcontrol com.1.1

Port          Flow
------------  --------
com.1.1       ctsrts
```

set console flowcontrol

Use this command to set the type of flow control for one or more console ports.

Syntax

set console flowcontrol {**none** | **ctsrts** | **dsrdtr**} [*port-string*]

Parameters

none	Disables all hardware flow control.
ctsrts	Enables CTS/RTS (Clear to Send/Request to Send) hardware flow control.
dsrdtr	Enables DSR/DTR (Data Set Ready/Data Terminal Ready) hardware flow control.
port-string	(Optional) Sets flow control for specific console port(s).

Defaults

If *port-string* is not specified, flow control will be set for all console ports.

Mode

Switch command, Read-Write.

Example

This example shows how to enable DSR/DTR flow control for console port com.1.1:

```
Matrix(rw)->set console flowcontrol dsrdtr com.1.1
```

clear console flowcontrol

Use this command to clear the type of flow control for one or more console ports.

Syntax

clear console flowcontrol [*port-string*]

Downloaded from www.Manualslib.com manuals search engine

Parameters

port-string	(Optional) Clears flow control for specific console port(s).

Defaults

If *port-string* is not specified, flow control will be cleared for all console ports.

Mode

Switch command, Read-Write.

Example

This example shows how to clear flow control for console port com.1.1:

```
Matrix(rw)->clear console flowcontrol com.1.1
```

show console bits

Use this command to display the number of bits per character set for one or more console ports.

Syntax

show console bits [*port-string*]

Parameters

port-string	(Optional) Displays the bits per character setting for specific console port(s).

Defaults

If *port-string* is not specified, the bits per character setting for all console ports will be displayed.

Mode

Switch command, Read-Only.

Example

This example shows how to display the bits per character setting for console port com.1.1:

```
Matrix(rw)->show console bits com.1.1
Port          Bits
------------  --------
com.1.1       8
```

set console bits

Use this command to set the number of bits per character for one or more console ports.

Syntax

set console bits *num-bits* [*port-string*]

Downloaded from www.Manualslib.com manuals search engine

Parameters

num-bits	Specifies the number of bits per character. Valid values are **5**, **6**, **7**, and **8**.
port-string	(Optional) Sets bits per character for specific console port(s).

Defaults

If *port-string* is not specified, bits per character will be set for all console ports.

Mode

Switch command, Read-Write.

Example

This example shows how to set bits per character to 5 for console port com.1.1:

```
Matrix(rw)->set console bits 5 com.1.1
```

clear console bits

Use this command to clear the number of bits per character for one or more console ports.

Syntax

clear console bits [*port-string*]

Parameters

port-string	(Optional) Clears bits per character for specific console port(s).

Defaults

If *port-string* is not specified, bits per character will be cleared for all console ports.

Mode

Switch command, Read-Write.

Example

This example shows how to clear bits per character for console port com.1.1:

```
Matrix(rw)->clear console bits com.1.1
```

show console stopbits

Use this command to display the console port stop bits per character.

Syntax

show console stopbits [*port-string*]

Parameters

port-string	(Optional) Displays stop bits for specific console port(s).

Downloaded from www.Manualslib.com manuals search engine

Defaults

If *port-string* is not specified, stop bits per character will be displayed for all console ports.

Mode

Switch command, Read-Write.

Example

This example shows how to show stop bits per character on com.1.1:

```
Matrix(rw)->show console stopbits com.1.1
Port          StopBits
------------  --------
com.1.1       one
```

set console stopbits

Use this command to set the stop bits per character for one or more console ports.

Syntax

set console stopbits {**one** | **oneandhalf** | **two**} [*port-string*]

Parameters

one | **oneandhalf** | **two**	Sets stop bits per character to 1, 1.5 or 2.
port-string	(Optional) Sets stop bits for specific console port(s).

Defaults

If *port-string* is not specified, stop bits per character will be set for all console ports.

Mode

Switch command, Read-Write.

Example

This example shows how to set stop bits per character to 2 for console port com.1.1:

```
Matrix(rw)->set console stopbits 2 com.1.1
```

clear console stopbits

Use this command to clear the stop bits per character for one or more console ports.

Syntax

clear console stopbits [*port-string*]

Parameters

port-string	(Optional) Clears stop bits for specific console port(s).

Downloaded from www.Manualslib.com manuals search engine

Defaults

If *port-string* is not specified, stop bits per character will be cleared for all console ports.

Mode

Switch command, Read-Write.

Example

This example shows how to clear stop bits per character for console port com.1.1:

```
Matrix(rw)->clear console stopbits com.1.1
```

show console parity

Use this command to display the type of parity checking set for one or more console ports.

Syntax

show console parity [*port-string*]

Parameters

port-string	(Optional) Displays parity type for specific console port(s).

Defaults

If *port-string* is not specified, parity type for all console ports will be displayed.

Mode

Switch command, Read-Only.

Example

This example shows how to display parity type for console port com.1.1:

```
Matrix(rw)->show console parity com.1.1

Port          Parity
------------  --------
com.1.1       none
```

set console parity

Use this command to set the parity type for one or more console ports.

Syntax

set console parity {**none** | **odd** | **even** | **mark** | **space**} [*port-string*]

Parameters

none	Specifies that no parity checking will be performed.
odd	Enables odd parity checking.

Downloaded from www.Manualslib.com manuals search engine

even	Enables even parity checking.
mark	Enables mark parity checking.
space	Enables space parity checking.
port-string	(Optional) Sets parity type for specific console port(s).

Defaults

If *port-string* is not specified, parity type will be set for all console ports.

Mode

Switch command, Read-Write.

Example

This example shows how to enable even parity checking on console port com.1.1:

```
Matrix(rw)->set console parity even com.1.1
```

clear console parity

Use this command to clear the parity type for one or more console ports.

Syntax

clear console parity [*port-string*]

Parameters

port-string	(Optional) Clears the parity type for specific console port(s).

Defaults

If *port-string* is not specified, parity type will be cleared for all console ports.

Mode

Switch command, Read-Write.

Example

This example shows how to clear parity type on console port com.1.1:

```
Matrix(rw)->clear console parity com 1.1
```


Downloaded from www.Manualslib.com manuals search engine

Reviewing Port Status

Purpose

To display operating status, duplex mode, speed, port type, and statistical information about traffic received and transmitted through one or all switch ports on the device.

Commands

The commands used to review port status are listed below and described in the associated sections as shown.

For information about...	Refer to page...
show port	4-13
show port status	4-14
show port counters	4-15
show port operstatuscause	4-17
clear port operstatuscause	4-18

show port

Use this command to display whether or not one or more ports are enabled for switching.

Syntax

show port [*port-string*]

Parameters

port-string	(Optional) Displays operational status for specific port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.

Defaults

If *port-string* is not specified, operational status information for all ports will be displayed.

Mode

Switch command, Read-Only.

Examples

This example shows how to display operational status information for 1-Gigabit Ethernet port 14 in module 3:

```
Matrix(rw)->show port ge.3.14
Port ge.3.14 enabled
```


Downloaded from www.Manualslib.com manuals search engine

show port status

Use this command to display operating and admin status, speed, duplex mode and port type for one or more ports on the device.

Syntax

show port status [*port-string*] [**-interesting**]

Parameters

port-string	(Optional) Displays status for specific port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.
-interesting	(Optional) Displays only ports with an operational status of up or dormant.

Defaults

If no options are specified, status information for all ports will be displayed.

Mode

Switch command, Read-Only.

Examples

This example shows how to display status information for port ge.3.1 through 4:

```
Matrix(rw)->show port status ge.3.1-4

Port           Alias           Oper      Admin    Speed     Duplex   Type
               (truncated)      Status   Status
------------  --------------  -------  -------  --------  -------  -------------
ge.3.14                       up        up      1 Gbps    full     1000-SX MT-RJ
```

This example shows how to display status information for console ports:

```
Matrix(rw)->show port status com.*.*

Port           Alias           Oper     Admin     Speed     Duplex   Type
               (truncated)     Status   Status
------------  --------------  -------  -------  --------  -------  -------------
com.5.1                       up       up        38 Kbps            RS232   RJ45
com.7.1                       up       up        38 Kbps            RS232   RJ45
```

Table 4-1 provides an explanation of the command output.

Table 4-1 show port status Output Details

Output...	What it displays...
Port	Port designation. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.
Alias (truncated)	Alias configured for the port. For details on using the **set port alias** command, refer to "show port alias" on page 4-21.

Downloaded from www.Manualslib.com manuals search engine

Table 4-1 show port status Output Details

Output...	What it displays...
Oper Status	Operating status (up or down).
Admin Status	Whether the specified port is enabled (up) or disabled (down). For details on using the **set port disable** command to change the default port status of enabled, refer to "set port disable" on page 4-20. For details on using the **set port enable** command to re-enable ports, refer to "set port enable" on page 4-21.
Speed	Operational speed in Mbps or Kbps of the specified port. For details on using the **set port speed** command to change defaults, refer to "set port speed" on page 4-25.
Duplex	Duplex mode (half or full) of the specified port. For details on using the **set port duplex** command to change defaults, refer to "Setting Auto-Negotiation and Advertised Ability" on page 4-30.
Type	Physical port and interface type.

show port counters

Use this command to display port counter statistics detailing traffic through the device and through all MIB2 network devices.

Syntax

show port counters [*port-string*] [**switch** | **mib2**]

Parameters

port-string	(Optional) Displays counter statistics for specific port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.
switch | **mib2**	(Optional) Displays switch or MIB2 statistics. Switch statistics detail performance of the Matrix switch device. MIB2 interface statistics detail performance of all network devices.

Defaults

- If *port-string* is not specified, counter statistics will be displayed for all ports.
- If **mib2** or **switch** are not specified, all counter statistics will be displayed for the specified port(s).

Mode

Switch command, Read-Only.

Examples

This example shows how to display all counter statistics, including MIB2 network traffic and traffic through the device for fe.3.1:

```
Matrix(rw)->show port counters fe.3.1


Port: fe.3.1   MIB2 Interface: 1   Bridge Port: 2
```


Downloaded from www.Manualslib.com manuals search engine

```
No counter discontinuity time
------------------------------------------------------------------

MIB2 Interface Counters
-----------------------
In Octets                          0
In Unicast Pkts                    0
In Multicast Pkts                  0
In Broadcast Pkts                  0
In Discards                        0
In Errors                          0
In Unknown Protocol                0
Out Octets                         0
Out Unicasts Pkts                  0
Out Multicast Pkts                 0
Out Broadcast Pkts                 0
Out Errors                         0
Out Queue Length                   256

802.1Q Switch Counters
----------------------
Frames Received                    0
Frames Transmitted                 0
Frames Filtered                    0
```

This example shows how to display all fe.3.1 port counter statistics related to traffic through the device.

```
Matrix(rw)->show port counters fe.3.1 switch

Port: fe.3.1   Bridge Port: 2
No counter discontinuity time
802.1Q Switch Counters
-----------------------------------------
Frames Received                        0
Frames Transmitted                     0
Frames Filtered                        0
```

Table 4-2 provides an explanation of the command output.

Table 4-2 show port counters Output Details

Output...	What it displays...
Port	Port designation. For a detailed description of possible *port-string* values, refer to “Port String Syntax Used in the CLI” on page 4-2.
MIB2 Interface	MIB2 interface designation.
Bridge Port	IEEE 802.1D bridge port designation.

Downloaded from www.Manualslib.com manuals search engine

Table 4-2 show port counters Output Details

Output...	What it displays...
MIB2 Interface Counters	MIB2 network traffic counts
802.1Q Switch Counters	Counts of frames received, transmitted, and filtered.

show port operstatuscause

Use this command to display the causes configured to place operating status to a down or dormant state for one or more ports.

Syntax

show port operstatuscause [*port-string*] [**any**] [**modifiable**][**admin**] [**linkloss**] [**linkflap**] [**self**] [**init**] [**flowlimit**] [**policy**] [**cos**] [**dot1x**] [**lag**]

Parameters

port-string	(Optional) Displays causes for specific port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.
any	(Optional) Displays a table of all causes.
modifiable	(Optional) Displays a table of modifiable causes.
admin	(Optional) Displays ports down due to adminStatus.
linkloss	(Optional) Displays ports down due to link loss.
linkflap	(Optional) Displays ports down due to link flap violation. For more information on configuring the link flap function, refer to "Configuring Link Traps and Link Flap Detection" on page 4-39.
self	(Optional) Displays ports down due to a hardware cause.
init	(Optional) Displays ports in initialization phase.
flowlimit	(Optional) Displays ports down due to a flow limiting constraint. For more information on configuring flow limiting, which is also known as flow setup throttling, refer to "Configuring Flow Setup Throttling (FST)" on page 24-25.
policy	(Optional) Displays ports down due to policy restriction. For more information on configuring user policies, refer to Chapter 8.
cos	(Optional) Displays ports down due to Class of Service constraint. For more information on configuring Class of Service, refer to "Configuring Policy Class of Service (CoS)" on page 8-21.
dot1x	(Optional) Displays ports dormant due to 802.1X enforcement. For more information on configuring 802.1X, refer to "Configuring 802.1X Authentication" on page 25-2.
lag	(Optional) Displays ports dormant due to Link Aggregation Group (LAG) membership. For more information on configuring LAG, refer to "Configuring Link Traps and Link Flap Detection" on page 4-39.

Defaults

If no options are specified, causes for all ports will be displayed.

Downloaded from www.Manualslib.com manuals search engine

Mode

Switch command, Read-Only.

Example

This example shows how to display operation status causes for ports ge.1.1 through 6. In this case, port ge.1.6 is down due to a link loss:

```
Matrix(rw)->show port operstatuscause ge.1.1-6
          +------------------------------+
          | A  L  L                 D    |
          | D  L  F  S  I  F        O    |
          | M  O  L  E  N  L  P  C  T  L |
          | I  S  A  L  I  O  O  O  1  A |
Port      | N  S  P  F  T  W  L  S  X  G |
----------+------------------------------+
ge.1.1    | .  .  .  .  .  .  .  .  .  . |
ge.1.2    | .  .  .  .  .  .  .  .  .  . |
ge.1.3    | .  .  .  .  .  .  .  .  .  . |
ge.1.4    | .  .  .  .  .  .  .  .  .  . |
ge.1.5    | .  .  .  .  .  .  .  .  .  . |
ge.1.6    | .  X  .  .  .  .  .  .  .  . |
```

clear port operstatuscause

Use this command to override the causes configured to place operating status to a down or dormant state for one or more ports.

Syntax

clear port operstatuscause [*port-string*] [**admin**] [**linkflap**] [**flowlimit**] [**policy**] [**cos**][**all**]

Parameters

port-string	(Optional) Overrides causes for specific port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.
admin	(Optional) Resets adminStatus to up.
linkflap	(Optional) Overrides link flap violation status.
flowlimit	(Optional) Overrides a flow limiting constraint.
policy	(Optional) Overrides a policy restriction.
cos	(Optional) Overrides a Class of Service constraint.
all	(Optional) Overrides all modifiable operStatus down causes.

Defaults

If no options are specified, all operating status causes will be overridden for all ports.

Downloaded from www.Manualslib.com manuals search engine

Mode

Switch command, Read-Write.

Example

This example shows how to override all operational causes on all ports:

```
Matrix(rw)->clear port operstatuscause
```


Downloaded from www.Manualslib.com manuals search engine

Disabling / Enabling and Naming Ports

Purpose

To disable and re-enable one or more ports, and to assign an alias to a port. By default, all ports are enabled at device startup. You may want to disable ports for security or to troubleshoot network issues.

Commands

For information about...	Refer to page...
set port disable	4-20
set port enable	4-21
show port alias	4-21
set port alias	4-22
show forcelinkdown	4-22
set forcelinkdown	4-23
clear forcelinkdown	4-23

set port disable

Use this command to administratively disable one or more ports.

Syntax

set port disable *port-string*

Parameters

port-string	Specifies the port(s) to disable. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to disable Fast Ethernet port 1 in module1:

```
Matrix(rw)->set port disable fe.1.1
```


Downloaded from www.Manualslib.com manuals search engine

set port enable

Use this command to administratively enable one or more ports.

Syntax

set port enable *port-string*

Parameters

port-string	Specifies the port(s) to enable. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to enable Fast Ethernet port 3 in module1:

```
Matrix(rw)->set port enable fe.1.3
```

show port alias

Use this command to display alias name(s assigned to one or more ports.

Syntax

show port alias [*port-string*]

Parameters

port-string	(Optional) Displays alias name(s) for specific port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.

Defaults

If *port-string* is not specified, aliases for all ports will be displayed.

Mode

Switch command, Read-Only.

Example

This example shows how to display alias information for fe.3.1. In this case, an alias has not been assigned:

```
Matrix(rw)->show port alias fe.3.1
Alias not assigned on port fe.3.1.
```


Downloaded from www.Manualslib.com manuals search engine

set port alias

Use this command to assign an alias name to a port.

Syntax

set port alias *port-string* [*string*]

Parameters

port-string	Specifies the port to which an alias will be assigned. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.
string	(Optional) Assigns a text string name to the port.

Defaults

If *string* is not specified, the alias assigned to the port will be cleared.

Mode

Switch command, Read-Write.

Example

This example shows how to assign the alias "management" to fe.3.1:

```
Matrix(rw)->set port alias fe.3.1 management
```

show forcelinkdown

Use this command to display the status of the force link down function.

Syntax

show forcelinkdown

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Only.

Example

This example shows how to display the status of the force link down function:

```
Matrix(rw)->show forcelinkdown
ForceLinkDown feature is globally enabled
```


Downloaded from www.Manualslib.com manuals search engine

set forcelinkdown

Use this command to enable or disable the force link down function. When enabled, this forces ports in the “operstatus down” state to become disabled.

Syntax

```
set forcelinkdown {enable | disable}
```

Parameters

enable | **disable**	Enables or disables the force link down function on all ports.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to enable the force link down function:

```
Matrix(rw)->set forcelinkdown enable
```

clear forcelinkdown

Use this command to resets the force link down function to the default state of disabled.

Syntax

```
clear forcelinkdown
```

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to reset the force link down function to disabled:

```
Matrix(rw)->clear forcelinkdown
```


Downloaded from www.Manualslib.com manuals search engine

Setting Speed and Duplex Mode

Purpose

To review and set the operational speed in Mbps and the default duplex mode: **Half**, for half duplex, or **Full**, for full duplex for one or more ports.



Note: These settings only take effect on ports that have auto-negotiation disabled.

Commands

For information about...	Refer to page...
show port speed	4-24
set port speed	4-25
show port duplex	4-25
set port duplex	4-26

show port speed

Use this command to display the default speed setting on one or more ports.

Syntax

show port speed [*port-string*]

Parameters

port-string	(Optional) Displays default speed setting(s) for specific port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.

Defaults

If *port-string* is not specified, default speed settings for all ports will display.

Mode

Switch command, Read-Only.

Example

This example shows how to display the default speed setting for 1-Gigabit Ethernet port 14 in module 3:

```
Matrix(rw)->show port speed ge.3.14
default speed is 1000 on port ge.3.14.
```


Downloaded from www.Manualslib.com manuals search engine

set port speed

Use this command to set the default speed of one or more ports. This setting only takes effect on ports that have auto-negotiation disabled.

Syntax

set port speed *port-string* {**10** | **100** | **1000**}

Parameters

port-string	Specifies the port(s) for which to a speed value will be set. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.
10 | **100** | **1000**	Specifies the port speed. Valid values are: **10** Mbps, **100** Mbps, or **1000** Mbps.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to set Fast Ethernet port 3 in module3 to a port speed of 10 Mbps:

```
Matrix(rw)->set port speed fe.3.3 10
```

show port duplex

Use this command to display the default duplex setting (half or full) for one or more ports.

Syntax

show port duplex [*port-string*]

Parameters

port-string	(Optional) Displays default duplex setting(s) for specific port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.

Defaults

If *port-string* is not specified, default duplex settings for all ports will be displayed.

Mode

Switch command, Read-Only.

Downloaded from www.Manualslib.com manuals search engine

Example

This example shows how to display the default duplex setting for 1-Gigabit Ethernet port 14 in module 3:

```
Matrix(rw)->show port duplex ge.3.14
default duplex mode is full on port ge.3.14.
```

set port duplex

Use this command to set the default duplex type for one or more ports.

Syntax

set port duplex *port-string* {**full** | **half**}

Parameters

port-string	Specifies the port(s) for which duplex type will be set. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.
full | **half**	Sets the port(s) to full-duplex or half-duplex operation.

Defaults

None.

Mode

Switch command, Read-Write.

Usage

This command will only take effect on ports that have auto-negotiation disabled.

Example

This example shows how to set Fast Ethernet port 17 in module 1 to full duplex:

```
Matrix(rw)->set port duplex fe.1.17 full
```


Downloaded from www.Manualslib.com manuals search engine

Enabling / Disabling Jumbo Frame Support

Purpose

To review, enable, and disable jumbo frame support on one or more ports. This allows Gigabit Ethernet ports to transmit frames up to 10 KB in size.

Commands

For information about...	Refer to page...
show port jumbo	4-27
set port jumbo	4-28
clear port jumbo	4-28

show port jumbo

Use this command to display the status of jumbo frame support and maximum transmission units (MTU) on one or more ports.

Syntax

show port jumbo [*port-string*]

Parameters

port-string	(Optional) Displays the status of jumbo frame support for specific port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.

Defaults

If *port-string* is not specified, jumbo frame support status for all ports will display.

Mode

Switch command, Read-Only.

Example

This example shows how to display the status of jumbo frame support for ge.1.1:

```
Matrix(rw)->show port jumbo ge.1.1

Port Number  Jumbo Oper Status  Jumbo Admin Status  Jumbo MTU
-----------  -----------------  ------------------  ---------
ge.1.1       Disabled           Disabled            10239
```


Downloaded from www.Manualslib.com manuals search engine

set port jumbo

Use this command to enable or disable jumbo frame support on one or more ports.

Syntax

set port jumbo {**enable** | **disable**} [*port-string*]

Parameters

enable | **disable**	Enables or disables jumbo frame support.
port-string	(Optional) Specifies the port(s) on which to disable or enable jumbo frame support. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.

Defaults

If *port-string* is not specified, jumbo frame support will be enabled or disabled on all ports.

Mode

Switch command, Read-Write.

Usage

By default, jumbo frame support is disabled on all ports and path MTU discovery is enabled. When jumbo frame support is enabled, path MTU discovery should not be disabled. For details on setting the path MTU state, refer to "set mtu" on page 2-91.

Examples

This example shows how to enable jumbo frame support for 1-Gigabit Ethernet port 14 in module 3:

```
Matrix(rw)->set port jumbo enable ge.3.14
```

This example shows how to enable jumbo frame support for router in slot 2, router instance 1.:

```
Matrix(rw)->set port jumbo enable rtr.2.1
```

clear port jumbo

Use this command to reset jumbo frame support status to enabled on one or more ports.

Syntax

clear port jumbo [*port-string*]

Parameters

port-string	(Optional) Specifies the port(s) on which to reset jumbo frame support status to enabled. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.

Defaults

If *port-string* is not specified, jumbo frame support status will be reset on all ports.

Downloaded from www.Manualslib.com manuals search engine

Mode

Switch command, Read-Write.

Example

This example shows how to reset jumbo frame support status for 1-Gigabit Ethernet port 14 in module 3:

```
Matrix(rw)->clear port jumbo ge.3.14
```


Downloaded from www.Manualslib.com manuals search engine

Setting Auto-Negotiation and Advertised Ability

Purpose

To review, disable or enable auto-negotiation, and to review or set a port's advertised mode of operation.

During auto-negotiation and advertised ability, the port "tells" the device at the other end of the segment what its capabilities and mode of operation are. If auto-negotiation is disabled, the port reverts to the values specified by default speed, default duplex, and the port flow control commands.

In normal operation, with all capabilities enabled, advertised ability enables a port to "advertise" that it has the ability to operate in any mode. The user may choose to configure a port so that only a portion of its capabilities are advertised and the others are disabled.



Note: Advertised ability can be activated only on ports that have auto-negotiation enabled.

Commands

For information about...	Refer to page...
show port negotiation	4-30
set port negotiation	4-31
show port mdix	4-31
set port mdix	4-32
clear port mdix	4-33
show port advertise	4-33
set port advertise	4-34
clear port advertise	4-35

show port negotiation

Use this command to display the status of auto-negotiation for one or more ports.

Syntax

show port negotiation [*port-string*]

Parameters

port-string	(Optional) Displays auto-negotiation status for specific port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.

Defaults

If *port-string* is not specified, auto-negotiation status for all ports will be displayed.

Downloaded from www.Manualslib.com manuals search engine

Mode

Switch command, Read-Only.

Example

This example shows how to display auto-negotiation status for 1-Gigabit Ethernet port 14 in module 3:

```
Matrix(rw)->show port negotiation ge.3.14
auto-negotiation is enabled on port ge.3.14.
```

set port negotiation

Use this command to enable or disable auto-negotiation on one or more ports.

Syntax

set port negotiation *port-string* {**enable** | **disable**}

Parameters

port-string	Specifies the port(s) for which to enable or disable auto-negotiation. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.
enable | **disable**	Enables or disables auto-negotiation.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to disable auto-negotiation on 1-Gigabit Ethernet port 3 in module 14:

```
Matrix(rw)->set port negotiation ge.3.14 disable
```

show port mdix

Use this command to display the MDI/MDIX mode on one or more ports. This function detects and adapts to straight through (MDI) or cross-over (MDIX) Ethernet cabling on switch ports.

Syntax

show port mdix [*port-string*] {**all** | **auto** | **mdi** | **mdix**}

Parameters

port-string	(Optional) Displays mode for specific port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.
all	Displays port(s) MDI and MDIX admin status.

Downloaded from www.Manualslib.com manuals search engine

auto	Displays port(s) automatically determining MDI/MDIX.
mdi	Displays port(s) forced to MDI configuration.
mdix	Displays port(s) forced to MDIX configuration.

Defaults

If *port-string* is not specified, the mode for all ports will be displayed.

Mode

Switch command, Read-Only.

Example

This example shows how to display MDI/MDIX mode for 1-Gigabit Ethernet port 14 in module 3:

```
Matrix(rw)->show port negotiation ge.3.14
mdix configuration is auto on port fe.3.14
```

set port mdix

Use this command to set MDI/MDIX mode on one or more ports.

Syntax

set port mdix [*port-string*] {**auto** | **mdi** | **mdix**}

Parameters

port-string	(Optional) Sets mode for specific port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.
auto	Sets port(s) to automatically determine MDI/MDIX.
mdi	Forces port(s) to MDI configuration.
mdix	Forces port(s) to MDIX configuration.

Defaults

If *port-string* is not specified, mode will be set for all ports.

Mode

Switch command, Read-Write.

Example

This example shows how to force 1-Gigabit Ethernet port 14 in module 3 to MDIX configuration:

```
Matrix(rw)->set port mdix ge.3.14 mdix
```


Downloaded from www.Manualslib.com manuals search engine

clear port mdix

Use this command to reset MDIX mode to the default setting of auto on one or more ports.

Syntax

clear port mdix [*port-string*]

Parameters

port-string	(Optional) Resets mode for specific port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.

Defaults

If *port-string* is not specified, mode will be reset for all ports.

Mode

Switch command, Read-Write.

Example

This example shows how to reset 1-Gigabit Ethernet port 14 in module 3 to auto MDI/MDIX configuration:

```
Matrix(rw)->set port mdix ge.3.14
```

show port advertise

Use this command to display the advertised ability on one or more ports.

Syntax

show port advertise [*port-string*]

Parameters

port-string	(Optional) Displays advertised ability for specific port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.

Defaults

If *port-string* is not specified, advertised ability for all ports will be displayed.

Mode

Switch command, Read-Only.

Example

This example shows how to display advertised ability fe.1.16:

```
Matrix(rw)->show port advertise fe.1.16
fe.1.16      capability   advertised    remote
---------------------------------------------
```


Downloaded from www.Manualslib.com manuals search engine

```
10BASE-T          yes         yes         no
10BASE-TFD        yes         yes         no
100BASE-TX        yes         yes         no
100BASE-TXFD      yes         yes         no
1000BASE-X        no          no          no
1000BASE-XFD      no          no          no
1000BASE-T        no          no          no
1000BASE-TFD      no          no          no
other             no          no          yes
pause             yes         yes         no
Apause            no          no          no
Spause            no          no          no
Bpause            no          no          no
```

Table 4-3 provides an explanation of the command output.

Table 4-3 show port advertise Output Details

Output...	What it displays...
capability	Whether or not the port is capable of operating in the following modes: • **10t** - 10BASE-T half duplex mode • **10tfd** - 10BASE-T full duplex mode • **100tx** - 100BASE-TX half duplex mode • **100txfd** - 100BASE-TX full duplex mode • **1000x** - 1000BASE-X, -LX, -SX, -CX half duplex mode • **1000xfd** - 1000BASE-X, -LX, -SX, -CX full duplex mode • **1000t** - 1000BASE-T half duplex mode • **1000tfd** - 1000BASE-T full duplex mode • **other** - Other modes. • **pause** - PAUSE for full-duplex links • **apause** - Asymmetric PAUSE for full-duplex links • **spause** - Symmetric PAUSE for full-duplex links • **bpause** - Asymmetric and Symmetric PAUSE for full-duplex links
advertised	Whether or not the port is configured to advertise it is capable of operating in the modes listed.
remote	Whether this port's link partner is advertising the listed mode.

set port advertise

Use this command to enable or disable and to configure the advertised ability on one or more ports.

Syntax

set port advertise *port-string* [**10t**] [**10tfd**] [**100tx**] [**100txfd**] [**1000x**] [**1000xfd**] [**1000t**] [**1000tfd**] [**pause**] [**apause**] [**spause**] [**bpause**]

Downloaded from www.Manualslib.com manuals search engine

Parameters

port-string	Specifies the port(s) for which to set advertised ability. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.
10t	(Optional) Advertises 10BASE-T half duplex mode.
10tfd	(Optional) Advertises 10BASE-T full duplex mode.
100tx	(Optional) Advertises 100BASE-TX half duplex mode.
100txfd	(Optional) Advertises 100BASE-TX full duplex mode.
1000x	(Optional) Advertises 1000BASE-X, -LX, -SX, -CX half duplex mode.
1000xfd	(Optional) Advertises 1000BASE-X, -LX, -SX, -CX full duplex mode.
1000t	(Optional) Advertises 1000BASE-T half duplex mode.
1000tfd	(Optional) Advertises 1000BASE-T full duplex mode.
pause	(Optional) Advertises PAUSE for full-duplex links.
apause	(Optional) Advertises asymmetric PAUSE for full-duplex links.
spause	(Optional) Advertises symmetric PAUSE for full-duplex links.
bpause	(Optional) Advertises asymmetric and symmetric PAUSE for full-duplex links

Defaults

At least one optional parameter must be specified.

Mode

Switch command, Read-Write.

Example

This example shows how to set fe.3.4 to advertise 100BASE-TX full duplex operation:

```
Matrix(rw)->set port advertise fe.3.4 100txfd
```

clear port advertise

Use this command to reset advertised ability to the default setting on one or more ports.

Syntax

clear port advertise *port-string* [**10t** | **10tfd** | **100tx** | **100txfd** | **1000x** | **1000txfd** | **1000t** | **1000tfd** | **pause** | **apause** | **spause** | **bpause**]

Parameters

port-string	Specifies port(s) for which advertised ability will be reset. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.
10t	(Optional) Clears 10BASE-T half duplex mode from the port's advertised ability.
10tfd	(Optional) Clears 10BASE-T full duplex mode from the port's advertised ability.

Downloaded from www.Manualslib.com manuals search engine

100tx	(Optional) Clears 100BASE-TX half duplex mode from the port's advertised ability.
100txfd	(Optional) Clears 100BASE-TX full duplex mode from the port's advertised ability.
1000x	(Optional) Clears 1000BASE-X, -LX, -SX, -CX half duplex mode from the port's advertised ability.
1000xfd	(Optional) Clears 1000BASE-X, -LX, -SX, -CX full duplex mode from the port's advertised ability.
1000t	(Optional) Clears 1000BASE-T half duplex mode from the port's advertised ability.
1000tfd	(Optional) Clears 1000BASE-T full duplex mode from the port's advertised ability.
pause	(Optional) Clears PAUSE for full-duplex links from the port's advertised ability.
apause	(Optional) Clears asymmetric PAUSE for full-duplex links from the port's advertised ability.
spause	(Optional) Clears symmetric PAUSE for full-duplex links from the port's advertised ability.
bpause	(Optional) Clears asymmetric and symmetric PAUSE for full-duplex links from the port's advertised ability.

Defaults

If not specified, all modes of advertised ability will be cleared.

Mode

Switch command, Read-Write.

Example

This example shows how to reset all advertised ability to default settings on fe.3.4:

```
Matrix(rw)->clear port advertise fe.3.4
```


Downloaded from www.Manualslib.com manuals search engine

Setting Flow Control

Purpose

To review, enable or disable port flow control. Flow control is used to manage the transmission between two devices as specified by IEEE 802.3x to prevent receiving ports from being overwhelmed by frames from transmitting devices.

Commands

For information about...	Refer to page...
show port flowcontrol	4-37
set port flowcontrol	4-38

show port flowcontrol

Use this command to display the flow control state for one or more ports.

Syntax

show port flowcontrol [*port-string*]

Parameters

port-string	(Optional) Displays flow control state for specific port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.

Defaults

If *port-string* is not specified, flow control information for all ports will be displayed.

Mode

Read-Only.

Example

This example shows how to display the port flow control state for fe.1.1-5:

```
Matrix(rw)->show port flowcontrol fe.1.1-5

Port         TX Admin  TX Oper RX Admin  RX Oper TX Pause Count RX Pause Count
------------ -------- -------- -------- -------- -------------- --------------
fe.1.1        enabled disabled  enabled disabled              0              0
fe.1.2        enabled disabled  enabled disabled              0              0
fe.1.3        enabled  enabled  enabled  enabled              0              0
fe.1.4        enabled disabled  enabled disabled              0              0
fe.1.5        enabled disabled  enabled disabled              0              0
```


Downloaded from www.Manualslib.com manuals search engine

Table 4-4 provides an explanation of the command output.

Table 4-4 show port flow control Output Details

Output...	What it displays...
Port	Port designation. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.
TX Admin	Whether or not the port is administratively **enabled** or **disabled** for sending flow control frames.
TX Oper	Whether or not the port is operationally **enabled** or **disabled** for sending flow control frames.
RX Admin	Whether or not the port is administratively **enabled** or **disabled** for acknowledging received flow control frames.
RX Oper	Whether or not the port is operationally **enabled** or **disabled** for acknowledging received flow control frames.
TX Pause Count	Number of Pause frames transmitted.
RX Pause Count	Number of Pause frames received.

set port flowcontrol

Use this command to enable or disable flow control settings for one or more ports.

Syntax

set port flowcontrol *port-string* {**receive** | **send** | **both**}{**enable** | **disable**}

Parameters

port-string	Specifies port(s) for which to enable or disable flow control. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.
receive | **send** | **both**	Enables or disables the port(s) to receive, send, or receive and send flow control packets.
enable | **disable**	Enables or disables flow control settings.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to enable ports fe.3.1 through 5 to send and receive flow control packets:

```
Matrix(rw)->set port flowcontrol fe.3.1-5 both enable
```


Downloaded from www.Manualslib.com manuals search engine

Configuring Link Traps and Link Flap Detection

Purpose

To disable or re-enable link traps and to configure the link flapping detection function. By default, all ports are enabled to send SNMP trap messages indicating changes in their link status (up or down). The link flap function detects when a link is going up and down rapidly (also called "link flapping") on a physical port, and takes the required actions (disable port, and eventually send notification trap) to stop such a condition. If left unresolved, the "link flapping" condition can be detrimental to network stability because it can trigger Spanning Tree and routing table recalculation.

Commands

For information about...	Refer to page...
show port trap	4-39
set port trap	4-40
show linkflap	4-40
set linkflap globalstate	4-43
set linkflap	4-43
set linkflap interval	4-44
set linkflap action	4-44
clear linkflap action	4-45
set linkflap threshold	4-45
set linkflap downtime	4-46
clear linkflap down	4-47
clear linkflap	4-47

show port trap

Use this command to display whether the port is enabled for generating an SNMP trap message if its link state changes.

Syntax

show port trap [*port-string*]

Parameters

port-string	(Optional) Displays link trap status for specific port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.

Defaults

If *port-string* is not specified, the trap status for all ports will be displayed.

Downloaded from www.Manualslib.com manuals search engine

Mode

Switch command, Read-Write.

Example

This example shows how to display link trap status for fe.3.1 through 4:

```
Matrix(rw)->show port trap fe.3.1-4
Link traps enabled on port fe.3.1.
Link traps enabled on port fe.3.2.
Link traps enabled on port fe.3.3.
Link traps enabled on port fe.3.4.
```

set port trap

Use this command to enable or disable ports for sending SNMP trap messages when their link status changes.

Syntax

set port trap *port-string* {**enable** | **disable**}

Parameters

port-string	Specifies the port(s) for which to enable or disable link trap messages. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.
enable | **disable**	Enables or disables link traps.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to disable link traps for Fast Ethernet port 3 in module3:

```
Matrix(rw)->set port trap fe.3.3 disable
```

show linkflap

Use this command to display link flap detection state and configuration information.

Syntax

show linkflap {**globalstate** | **portstate** | **parameters** | **metrics** | **portsupported** | **actsupported** | **maximum** | **downports** | **action** | **operstatus** | **threshold** | **interval**] | **downtime** | **currentcount** | **totalcount** | **timelapsed** | **violations** [*port-string*]}

Downloaded from www.Manualslib.com manuals search engine

Parameters

globalstate	Displays the global enable state of link flap detection.
portstate	Displays the port enable state of link flap detection.
parameters	Displays the current value of settable link flap detection parameters.
metrics	Displays linkflap detection metrics.
portsupported	Displays ports which can support the link flap detection function.
actsupported	Displays link flap detection actions supported by system hardware.
maximum	Displays the maximum allowed linkdowns per 10 seconds supported by system hardware.
downports	Displays ports disabled by link flap detection due to a violation.
action	Displays linkflap actions taken on violating port(s).
operstatus	Displays whether linkflap has deactivated port(s).
threshold	Displays the number of allowed link down transitions before action is taken.
interval	Displays the time period for counting link down transitions.
downtime	Displays how long violating port(s) are deactivated.
currentcount	Displays how many linkdown transitions are in the current interval.
totalcount	Displays how many linkdown transitions have occurred since the last reset.
timelapsed	Displays the time period since the last link down event or reset.
violations	Displays the number of link flap violations since the last reset.
port-string	(Optional) Displays information for specific port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.

Defaults

- If not specified, information about all link flap detection settings will be displayed.
- If *port-string* is not specified, information for all ports will be displayed.

Mode

Switch command, Read-Only.

Examples

This example shows how to display the global status of the link trap detection function:

```
Matrix(rw)->show linkflap globalstate
Linkflap feature globally disabled
```

This example shows how to display ports disabled by link flap detection due to a violation:

```
Matrix(rw)->show linkflap downports
Ports currently held DOWN for Linkflap violations:
None.
```

This example shows how to display the link flap parameters table:

```
Matrix(rw)->show linkflap parameters
```


Downloaded from www.Manualslib.com manuals search engine

```
Linkflap Port Settable Parameter Table (X means error occurred)
Port      LF Status  Actions  Threshold   Interval    Downtime
--------  ---------  -------  ----------  ----------  ----------
ge.1.1    disabled   .......  10          5           300
ge.1.2    enabled    D..S..T  3           5           300
ge.1.3    disabled   ...S..T  10          5           300
```

Table 4-5 provides an explanation of the **show linkflap parameters** command output.

Table 4-5 show linkflap parameters Output Details

Output...	What it displays...
Port	Port designation. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.
LF Status	Link flap enabled state.
Actions	Actions to be taken if the port violates allowed link flap behavior. D = disabled, S = Syslog entry will be generated, T= SNMP trap will be generated.
Threshold	Number of link down transitions necessary to trigger the link flap action.
Interval	Time interval (in seconds) for accumulating link down transitions.
Downtime	Interval (in seconds) port(s) will be held down after a link flap violation

This example shows how to display the link flap metrics table:

```
Matrix(rw)->show linkflap metrics
Port      LinkStatus   CurrentCount  TotalCount  TimeElapsed  Violations
--------  -----------  ------------  ----------  -----------  -------------
ge.1.1    operational  0             0           241437       0
ge.1.2    disabled     4             15          147          5
ge.1.3    operational  3             3           241402       0
```

Table 4-6 provides an explanation of the **show linkflap metrics** command output.

Table 4-6 show linkflap metrics Output Details

Output...	What it displays...
Port	Port designation. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.
LinkStatus	Link status according to the link flap function.
CurrentCount	Link down count accruing toward the link flap threshold.
TotalCount	Number of link downs since system start,
TimeElapsed	Time (in seconds) since the last link down event.
Violations	Number of link flap violations on listed ports since system start.

Downloaded from www.Manualslib.com manuals search engine

set linkflap globalstate

Use this command to globally enable or disable the link flap detection function. By default, the function is disabled globally and on all ports. If disabled globally after per-port settings have been configured using the commands later in this chapter, per-port settings will be retained.

Syntax

set linkflap globalstate {**disable** | **enable**}

Parameters

disable | **enable**	Globally disables or enables the link flap detection function.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to globally enable the link trap detection function:

```
Matrix(rw)->set linkflap globalstate enable
```

set linkflap

Use this command to enable or disable link flap monitoring on one or more ports.

Syntax

set linkflap portstate {**disable** | **enable**} [*port-string*]

Parameters

disable | **enable**	Disables or enables the link flap detection function.
port-string	(Optional) Specifies the port(s) on which to disable or enable monitoring. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.

Defaults

If *port-string* is not specified, all ports will be disabled or enabled.

Mode

Switch command, Read-Write.

Example

This example shows how to enable the link trap monitoring on all ports:

```
Matrix(rw)->set linkflap portstate enable
```


Downloaded from www.Manualslib.com manuals search engine

set linkflap interval

Use this command to set the time interval (in seconds) for accumulating link down transitions.

Syntax

set linkflap interval *port-string interval_value*

Parameters

port-string	Specifies the port(s) on which to set the link flap interval. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.
interval_value	Specifies an interval in seconds. A value of 0 will set the interval to forever.

Defaults

None.

Mode

Switch command, Read-Write.

Examples

This example shows how to set the link flap interval on port fe.1.4 to 1000 seconds:

```
Matrix(rw)->set linkflap interval fe.1.4 1000
```

set linkflap action

Use this command to set reactions to a link flap violation.

Syntax

set linkflap action *port-string* {**disableInterface** | **gensyslogentry** | **gentrap** | **all**}

Parameters

port-string	Specifies the port(s) on which to set the link flap action. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.
disableInterface | **gensyslogentry** | **gentrap** | **all**	Sets the reaction as: • Disabling the interface • Generating a Syslog entry • Generating an SNMP trap message, or • All of the above.

Defaults

None.

Downloaded from www.Manualslib.com manuals search engine

Mode

Switch command, Read-Write.

Examples

This example shows how to set the link flap violation action on port fe.1.4 to generating a Syslog entry:

```
Matrix(rw)->set linkflap action fe.1.4 gensyslogentry
```

clear linkflap action

Use this command to clear reactions to a link flap violation.

Syntax

clear linkflap action [*port-string*} {**disableInterface** | **gensyslogentry** | **gentrap** | **all**}

Parameters

port-string	(Optional) Specifies the port(s) on which to clear the link flap action. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.
disableInterface | **gensyslogentry** | **gentrap** | **all**	Clears the reaction of: • Disabling the interface • Generating a Syslog entry • Generating an SNMP trap message, or • All of the above.

Defaults

If *port-string* is not specified, actions will be cleared on all ports.

Mode

Switch command, Read-Write.

Examples

This example shows how to clear all link flap violation actions on all ports:

```
Matrix(rw)->clear linkflap action all
```

set linkflap threshold

Use this command to set the link flap action trigger count.

Syntax

set linkflap threshold *port-string threshold_value*

Downloaded from www.Manualslib.com manuals search engine

Parameters

port-string	Specifies the port(s) on which to set the link flap action trigger count. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.
threshold_value	Specifies the number of link down transitions necessary to trigger the link flap action.

Defaults

None.

Mode

Switch command, Read-Write.

Examples

This example shows how to set the link flap threshold on port fe.1.4 to 5:

```
Matrix(rw)->set linkflap threshold fe.1.4 5
```

set linkflap downtime

Use this command to set the time interval (in seconds) one or more ports will be held down after a link flap violation.

Syntax

set linkflap downtime *port-string downtime_value*

Parameters

port-string	Specifies the port(s) on which to set the link flap downtime. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.
downtime_value	Specifies a downtime in seconds. A value of 0 will set the downtime to forever.

Defaults

None.

Mode

Switch command, Read-Write.

Examples

This example shows how to set the link flap downtime on port fe.1.4 to 5000 seconds:

```
Matrix(rw)->set linkflap downtime fe.1.4 5000
```


Downloaded from www.Manualslib.com manuals search engine

clear linkflap down

Use this command to toggle link flap disabled ports to operational.

Syntax

clear linkflap down [*port-string*]

Parameters

port-string	Specifies the port(s) to make operational. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.

Defaults

If *port-string* is not specified, all ports disabled by a link flap violation will be made operational.

Mode

Switch command, Read-Write.

Examples

This example shows how to make disabled port fe.1.4 operational:

```
Matrix(rw)->clear linkflap down fe.1.4
```

clear linkflap

Use this command to clear all link flap options and / or statistics on one or more ports.

Syntax

clear linkflap {**all** | **stats** [*port-string*] | **parameter** *port-string* {**threshold** | **interval** | **downtime** | **all**}

Parameters

all | **stats**	Clears all options and statistics, or clears only statistics.
parameter	Clears link flap parameters.
threshold | **interval** | **downtime** | **all**	Clears link flap threshold, interval, downtime or all parameters.
port-string	(Optional unless parameter is specified) Specifies the port(s) on which to clear settings. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.

Defaults

If *port-string* is not specified, settings and/or statistics will be cleared on all ports.

Mode

Switch command, Read-Write.

Downloaded from www.Manualslib.com manuals search engine

Examples

This example shows how to clear all link flap options on port fe.1.4:

```
Matrix(rw)->clear linkflap all fe.1.4
```


Downloaded from www.Manualslib.com manuals search engine

Configuring Broadcast Suppression

Purpose

To review, disable or set the broadcast thresholds on one or more ports. This limits the amount of received broadcast frames that the specified port will be allowed to switch out to other ports. Broadcast suppression protects against broadcast storms, leaving more bandwidth available for critical data.

Commands

For information about...	Refer to page...
show port broadcast	4-49
set port broadcast	4-50
clear port broadcast	4-50

show port broadcast

Use this command to display port broadcast suppression information for one or more ports.

Syntax

show port broadcast [*port-string*]

Parameters

port-string	(Optional) Displays broadcast status for specific port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.

Defaults

If *port-string* is not specified, broadcast status of all ports will be displayed.

Mode

Read-Only.

Example

This example shows how to display broadcast information for Fast Ethernet port 2 in module 2:

```
Matrix(rw)->show port broadcast fe.2.2
Port          Total BC       Threshold       Peak Rate    Peak Rate Time
              Packets        (pkts/s)        (pkts/s)     (ddd:hh:mm:ss)
-------------------------------------------------------------------------
fe.2.2        165            148810          8            000:05:57:37
```

Table 4-7 provides an explanation of the command output.

Downloaded from www.Manualslib.com manuals search engine

Table 4-7 show port broadcast Output Details

Output...	What it displays...
Port	Port designation. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.
Total BC Packets	Total broadcast packets received on this port.
Threshold (pkts/s)	Current broadcast threshold in packets per second on this port.
Peak Rate (pkts/s)	Peak rate of broadcast transmission received on this port in packets per second.
Peak Rate Time (ddd:hh:mm:ss)	Time (in day, hours, minutes and seconds) the peak rate was reached on this port.

set port broadcast

Use this command to set the broadcast suppression limit, in packets per second, on one or more ports. This sets a threshold on the broadcast traffic that is received and switched out to other ports.

Syntax

set port broadcast *port-string threshold-val*

Parameters

port-string	Specifies the port(s) for which to set broadcast suppression. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.
threshold-val	Sets the packets per second threshold on broadcast traffic. Maximum value is 1488100 for Gigabit and 148810 for Fast Ethernet. If set to the maximum value, thresholding will be disabled.

Defaults

None.

Mode

Read-Write.

Example

This example shows how to set broadcast suppression to 800 packets per second on Fast Ethernet ports 1 through 5 in module 1:

```
Matrix(rw)->set port broadcast fe.1.1-5 800
```

clear port broadcast

Use this command to reset the broadcast threshold and/or clear the peak rate and peak time values on one or switch more ports.

Syntax

clear port broadcast *port-string* [**threshold**] [**peak**]

Downloaded from www.Manualslib.com manuals search engine

Parameters

port-string	Specifies the port(s) on which broadcast settings will be cleared. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.
threshold	(Optional) Clears the broadcast threshold setting.
peak	(Optional) Clears the broadcast peak rate and peak rate time values.

Defaults

If not specified, both **threshold** and **peak** settings will be cleared.

Mode

Read-Write.

Example

This example shows how to clear all broadcast suppression settings on Fast Ethernet ports 1 through 5 in module1:

```
Matrix(rw)->clear port broadcast fe.1.1-5 Setting Port Mirroring
```


Downloaded from www.Manualslib.com manuals search engine

Configuring Port Mirroring



Caution: Port mirroring configuration should be performed only by personnel who are knowledgeable about the effects of port mirroring and its impact on network operation.

The Matrix device allows you to mirror (or redirect) the traffic being switched on a port for the purposes of network traffic analysis and connection assurance. When port mirroring is enabled, one port becomes a monitor port for another port within the device.

Supported Mirrors

The following types of ports can participate in mirroring on the Matrix Series device:

- Physical ports, including front panel and FTM-1 ports
- Virtual ports, including Link Aggregation Group (LAG) and host ports. For details on configuring ports for link aggregation, refer to "Configuring LACP" on page 4-55.

Active Destination Port Configurations

Each Matrix DFE-Gold Series device supports three mirroring destination ports, which can be configured in a many-to-one mirroring configuration (that is, many destinations mirrored to one source port).



Note: Eight destination ports must be reserved for an IDS mirror.

Purpose

To review and configure port mirroring on the device.

Commands

For information about...	Refer to page...
show port mirroring	4-52
set port mirroring	4-53
clear port mirroring	4-54

show port mirroring

Use this command to display the source and target ports for mirroring, and whether mirroring is currently enabled or disabled for those ports.

Syntax

```
show port mirroring
```


Downloaded from www.Manualslib.com manuals search engine

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Only.

Example

This example shows how to display port mirroring information. In this case, fe.1.4 is configured as a source port and fe.1.11 is a target, but mirroring is not currently enabled between the ports:

```
Matrix(rw)->show port mirroring


Port Mirroring
==============
 Source Port = fe.1.4
 Target Port = fe.1.11
 Frames Mirrored = Rx and Tx
 Port Mirroring status disabled.
```

set port mirroring

Use this command to create a new mirroring relationship or to enable or disable an existing mirroring relationship between two ports.

Syntax

set port mirroring {**create** | **disable** | **enable**} | **igmp-mcast** {**enable** | **disable**} *source destination* [**both** | **rx** | **tx**]

Parameters

create | **disable** | **enable**	Creates, disables or enables mirroring settings on the specified ports.
igmp-mcast enable | **disable**	Enables or disables the mirroring of IGMP multicast frames.
source	Specifies the source port designation. This is the port on which the traffic will be monitored. For a description of port types that can participate in mirroring, refer to "Supported Mirrors" on page 4-52. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.
destination	Specifies the target port designation. This is the port that will duplicate or "mirror" all the traffic on the monitored port. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.
both | **rx** | **tx**	(Optional) Specifies that frames received and transmitted by the source port, only frames received, or only frames transmitted will be mirrored.

Downloaded from www.Manualslib.com manuals search engine

Defaults

If not specified, **both** received and transmitted frames will be mirrored.

Mode

Switch command, Read-Write.

Examples

This example shows how to enable port mirroring of transmitted and received frames with fe.1.4 as the source port and fe.1.11 as the target port:

```
Matrix(rw)->set port mirroring enable fe.1.4 fe.1.11 both
```

The following example command sequence creates a VLAN 1 and mirrors all VLAN 1 traffic, both inbound and outbound:

```
Matrix(rw)->set vlan interface 1 create
Matrix(rw)->set port mirroring create vlan.0.1 fe.1.1 both
```

clear port mirroring

Use this command to clear a port mirroring relationship.

Syntax

clear port mirroring {**igmp-mcast** | *source destination*}

Parameters

igmp-mcast	Clears IGMP multicast mirroring.
source	Specifies the source port of the mirroring configuration to be cleared. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.
destination	Specifies the target port of the mirroring configuration to be cleared.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to clear port mirroring between source port fe.1.4 and target port fe.1.11:

```
Matrix(rw)->clear port mirroring fe.1.4 fe.1.11
```


Downloaded from www.Manualslib.com manuals search engine

Configuring LACP

Caution: Link aggregation configuration should only be performed by personnel who are knowledgeable about Spanning Tree and Link Aggregation, and fully understand the ramifications of modifications beyond device defaults. Otherwise, the proper operation of the network could be at risk.

Using multiple links simultaneously to increase bandwidth is a desirable switch feature, which can be accomplished if both sides agree on a set of ports that are being used as a Link Aggregation Group (LAG). Once a LAG is formed from selected ports, problems with looping can be avoided since the Spanning Tree can treat this LAG as a single port.

Enabled by default on Matrix devices, the Link Aggregation Control Protocol (LACP) logically groups interfaces together to create a greater bandwidth uplink, or link aggregation, according to the IEEE 802.3ad standard. This standard allows the switch to determine which ports are in LAGs and configure them dynamically. Since the protocol is based on the IEEE 802.3ad specification, any switch from any vendor that supports this standard can aggregate links automatically.

802.3ad LACP aggregations can also be run to end-users (i.e., a server) or to a router.

Note: Earlier (proprietary) implementations of port aggregation referred to groups of aggregated ports as “trunks”.

LACP Operation

For each aggregatable port in the device, LACP:

- Maintains configuration information (reflecting the inherent properties of the individual links as well as those established by management) to control aggregation.
- Exchanges configuration information with other devices to allocate the link to a Link Aggregation Group (LAG).

Note: A given link is allocated to, at most, one Link Aggregation Group (LAG) at a time. The allocation mechanism attempts to maximize aggregation, subject to management controls.

- Attaches the port to the aggregator used by the LAG, and detaches the port from the aggregator when it is no longer used by the LAG.
- Uses information from the partner device’s link aggregation control entity to decide whether to aggregate ports.

The operation of LACP involves the following activities:

- Checking that candidate links can actually be aggregated.
- Controlling the addition of a link to a LAG, and the creation of the group if necessary.
- Monitoring the status of aggregated links to ensure that the aggregation is still valid.
- Removing a link from a LAG if its membership is no longer valid, and removing the group if it no longer has any member links.

In order to allow LACP to determine whether a set of links connect to the same device, and to determine whether those links are compatible from the point of view of aggregation, it is necessary to be able to establish

- A globally unique identifier for each device that participates in link aggregation.

Downloaded from www.Manualslib.com manuals search engine

- A means of identifying the set of capabilities associated with each port and with each aggregator, as understood by a given device.
- A means of identifying a LAG and its associated aggregator.

LACP Terminology

Table 4-8 defines key terminology used in LACP configuration.

Table 4-8 LACP Terms and Definitions

Term	Definition
Aggregator	Virtual port that controls link aggregation for underlying physical ports. Each Matrix Series module provides aggregator ports, which are designated in the CLI as **lag.0.1** through **lag.0.4**.
LAG	Link Aggregation Group. Once underlying physical ports (i.e.; **fe.x.x**, or **ge.x.x**) are associated with an aggregator port, the resulting aggregation will be represented as one LAG with a **lag.x.x** port designation.
LACPDU	Link Aggregation Control Protocol Data Unit. The protocol exchanges aggregation state/mode information by way of a port's actor and partner operational states. LACPDUs sent by the first party (the actor) convey to the second party (the actor's protocol partner) what the actor knows, both about its own state and that of its partner.
Actor and Partner	An actor is the local device sending LACPDUs. Its protocol partner is the device on the other end of the link aggregation. Each maintains current status of the other via LACPDUs containing information about their ports' LACP status and operational state.
Admin Key	Value assigned to aggregator ports and physical ports that are candidates for joining a LAG. The LACP implementation on Matrix Series devices will use this value to form an oper key and will determine which underlying physical ports are capable of aggregating by comparing oper keys. Aggregator ports allow only underlying ports with oper keys matching theirs to join their LAG.
System Priority	Value used to build a LAG ID, which determines aggregation precedence. If there are two partner devices competing for the same aggregator, LACP compares the LAG IDs for each grouping of ports. The LAG with the lower LAG ID is given precedence and will be allowed to use the aggregator. **Note:** Only one LACP system priority can be set on a Matrix Series device, using either the **set lacp asyspri** command ("set lacp asyspri" on page 4-60), or the **set port lacp** command ("set port lacp" on page 4-66).

Matrix Series Usage Considerations

In normal usage (and typical implementations) there is no need to modify any of the default LACP parameters on the Matrix Series device. The default values will result in the maximum number of aggregations possible. If the switch is placed in a configuration with its peers not running the protocol, no dynamic link aggregations will be formed and the switch will function normally (that is, will block redundant paths). For information about building static aggregations, refer to **set lacp static** ("set lacp static" on page 4-62).

Each Matrix Series module provides 4 virtual link aggregator ports, which are designated in the CLI as **lag.0.1** through **lag.0.4**. Once underlying physical ports (i.e.; **fe.x.x**, or **ge.x.x**) are associated with an aggregator port, the resulting aggregation will be represented as one LAG with a **lag.x.x** port designation. LACP determines which underlying physical ports are capable of aggregating

Downloaded from www.Manualslib.com manuals search engine

by comparing operational keys. Aggregator ports allow only underlying ports with keys matching theirs to join their LAG.

LACP uses a system priority value to build a LAG ID, which determines aggregation precedence. If there are two partner devices competing for the same aggregator, LACP compares the LAG IDs for each grouping of ports. The LAG with the lower LAG ID is given precedence and will be allowed to use the aggregator.

Note: Only one LACP system priority can be set on a Matrix Series device, using either the **set lacp asyspri** command ("set lacp asyspri" on page 4-60), or the **set port lacp** command ("set port lacp" on page 4-66).

There are a few cases in which ports will not aggregate:

- An underlying physical port is attached to another port on this same switch (loopback).
- There is no available aggregator for two or more ports with the same LAG ID. This can happen if there are simply no available aggregators, or if none of the aggregators have a matching admin key and system priority.
- 802.1x authentication is enabled, and ports that would otherwise aggregate are not 802.1X authorized.

The LACP implementation on the Matrix Series device will allow up to a maximum of four ports into a LAG. The device with the lowest LAG ID determines which underlying physical ports are allowed into a LAG based on the ports' LAG port priority. Ports with the lowest LAG port priority values are allowed into the LAG and all other speed groupings go into a standby state.

Note: To aggregate, underlying physical ports must be running in full duplex mode and must be of the same operating speed.

Purpose

To disable and re-enable the Link Aggregation Control Protocol (LACP), to display and configure LACP settings for one or more aggregator ports, and to display and configure the LACP settings for underlying physical ports that are potential members of a link aggregation.

Commands

For information about...	Refer to page...
show lacp	4-58
set lacp	4-59
clear lacp state	4-60
set lacp asyspri	4-60
set lacp aadminkey	4-61
clear lacp	4-61
set lacp static	4-62
clear lacp static	4-63
show lacp singleportlag	4-63
set singleportlag	4-64

Downloaded from www.Manualslib.com manuals search engine

For information about...	Refer to page...
clear singleportlag	4-64
show port lacp	4-65
set port lacp	4-66
clear port lacp	4-68
show lacp flowRegeneration	4-69
set lacp flowRegeneration	4-69
clear lacp flowRegeneration	4-70
show lacp outportAlgorithm	4-70
set lacp outportAlgorithm	4-71
clear lacp outportAlgorithm	4-71

show lacp

Use this command to display the global LACP enable state, or to display information about one or more aggregator ports.

Syntax

show lacp [**state** | *port-string*]

Parameters

state	(Optional) Displays the global LACP enable state.
port-string	(Optional) Displays LACP information for specific LAG port(s). Valid port designations are lag.0.1 - 4.

Defaults

- If **state** is not specified, aggregator information will be displayed for specified ports.
- If *port-string* is not specified, link aggregation information for all ports will be displayed.

Mode

Switch command, Read-Only.

Usage

Each Matrix Series module provides 4 virtual link aggregator ports, which are designated in the CLI as **lag.0.1** through **lag.0.4**. Once underlying physical ports (i.e.; **fe.x.x**, **ge.x.x**) are associated with an aggregator port, the resulting aggregation will be represented as one Link Aggregation Group (LAG) with a **lag.x.x** port designation.

Example

This example shows how to display information for aggregator port 4:

```
Matrix(rw)->show lacp lag.0.484


Aggregator:  lag.0.484
```


Downloaded from www.Manualslib.com manuals search engine

```
                          Actor                Partner
System Identifier:  00:e0:63:9d:b5:87      00:00:00:00:00:00
  System Priority:              32768                  32768
        Admin Key:              32768
         Oper Key:              32768                  32768
   Attached Ports:  None.
```

Table 4-9 provides an explanation of the command output.

Table 4-9 show lacp Output Details

Output...	What it displays...
Aggregator	LAG port designation. Each Matrix Series module provides 4 virtual link aggregator ports, which are designated in the CLI as **lag.0.1** through **lag.0.4**. Once underlying physical ports (i.e.; **fe.x.x**, **ge.x.x**) are associated with an aggregator port, the resulting Link Aggregation Group (LAG) is represented with a **lag.x.x** port designation.
Actor	Local device participating in LACP negotiation.
Partner	Remote device participating in LACP negotiation.
System Identifier	MAC addresses for actor and partner.
System Priority	System priority value which determines aggregation precedence. Only one LACP system priority can be set on a Matrix Series device, using either the **set lacp asyspri** command (“set lacp asyspri” on page 4-60), or the **set port lacp** command (“set port lacp” on page 4-66).
Admin Key	Port’s administratively assigned key.
Oper Key	Port’s operational key, derived from the admin key. Only underlying physical ports with oper keys matching the aggregator’s will be allowed to aggregate.
Attached Ports	Underlying physical ports associated with this aggregator. Matrix DFE-Gold Series devices allow for up to four ports per aggregator.

set lacp

Use this command to disable or enable the Link Aggregation Control Protocol (LACP) on the device. LACP is enabled by default.

Syntax

```
set lacp {disable | enable}
```

Parameters

disable | **enable**	Disables or enables LACP.

Defaults

None.

Downloaded from www.Manualslib.com manuals search engine

Mode

Switch command, Read-Write.

Example

This example shows how to disable LACP:

```
Matrix(rw)->set lacp disable
```

clear lacp state

Use this command to reset LACP to the default state of enabled.

Syntax

clear lacp state

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to reset LACP to enabled

```
Matrix(rw)->clear lacp state
```

set lacp asyspri

Use this command to set the LACP system priority.

Syntax

set lacp asyspri *value*

Parameters

asyspri	Sets the system priority to be used in creating a LAG (Link Aggregation Group) ID. Valid values are **0** to **65535**.
value	Specifies a system priority value. Valid values are **0** to **65535**, with precedence given to lower values.

Defaults

None.

Mode

Switch command, Read-Write.

Downloaded from www.Manualslib.com manuals search engine

Usage

Only one LACP system priority can be set on a Matrix Series device, using either this command, or the **set port lacp** command ("set port lacp" on page 4-66).

LACP uses this value to determine aggregation precedence. If there are two partner devices competing for the same aggregator, LACP compares the LAG IDs for each grouping of ports. The LAG with the lower LAG ID is given precedence and will be allowed to use the aggregator.

Example

This example shows how to set the LACP system priority to 1000:

```
Matrix(rw)->set lacp asyspri 1000
```

set lacp aadminkey

Use this command to set the administratively assigned key for one or more aggregator ports. LACP will use this value to form an oper key. Only underlying physical ports with oper keys matching those of their aggregators will be allowed to aggregate.

Syntax

set lacp aadminkey *port-string value*

Parameters

port-string	Specifies the LAG port(s) on which to assign an admin key.
value	Specifies an admin key value to set. Valid values are **0** to **65535**.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to set the LACP admin key to 2000 for LAG port 4:

```
Matrix(rw)->set lacp aadminkey lag.0.484 2000
```

clear lacp

Use this command to clear LACP system priority or admin key settings.

Syntax

clear lacp {[**asyspri**] [**aadminkey** *port-string*]}

Parameters

asyspri	Clears system priority.
aadminkey *port-string*	Clears admin keys for one or more ports.

Downloaded from www.Manualslib.com manuals search engine

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to clear the actor admin key for LAG port 4:

```
Matrix(rw)->clear lacp aadminkey lag.0.484
```

set lacp static

Use this command to assign one or more underlying physical ports to a Link Aggregation Group (LAG). Matrix DFE-Gold Series devices allow for up to four ports per aggregator.

Syntax

set lacp static *lagportstring* [*key*] *port-string*

Parameters

lagportstring	Specifies the LAG aggregator port to which new ports will be assigned.
key	(Optional) Specifies the new member port and LAG port aggregator admin key value. Only ports with matching keys are allowed to aggregate. Valid values are **0** - **65535**. **Note:** This key value must be unique. If ports other than the desired underlying physical ports share the same admin key value, aggregation will fail or undesired aggregations will form.
port-string	Specifies the member port(s) to add to the LAG. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.

Defaults

If not specified, a *key* will be assigned according to the specified aggregator. For example a key of 4 would be assigned to lag.0.4.

Mode

Switch command, Read-Write.

Usage

At least two ports need to be assigned to a LAG port for a Link Aggregation Group to form and attach to the specified LAG port.

The same usage considerations for dynamic LAGs discussed in "Matrix Series Usage Considerations" on page 4-56 apply to statically created LAGs.

Static LAG configuration should be performed by personnel who are knowledgeable about Link Aggregation. Misconfiguration can result in LAGs not being formed, or in ports attaching to the wrong LAG port, affecting proper network operation.

Downloaded from www.Manualslib.com manuals search engine

Example

This example shows how to add port fe.1.6 to the LAG of aggregator port 4:

```
Matrix(rw)->set lacp static lag.0.484 fe.1.6
```

clear lacp static

Use this command to remove specific ports from a Link Aggregation Group.

Syntax

clear lacp static *lagportstring port-string*

Parameters

lagportstring	Specifies the LAG aggregator port from which ports will be removed.
port-string	Specifies the port(s) to remove from the LAG. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to remove Fast Ethernet port 6 in module 1 from the LAG of aggregator port 4:

```
Matrix(rw)->clear lacp static lag.0.484 fe.1.6
```

show lacp singleportlag

Use this command to display the status of the single port LAG function.

Syntax

show lacp singleportlag

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Only.

Downloaded from www.Manualslib.com manuals search engine

Example

This example shows how to display the status of the single port LAG function:

```
Matrix(rw)->show lacp singleportlag
Single Port LAGs:              enabled
```

set singleportlag

Use this command to enable or disable the formation of single port LAGs. When enabled, this maintains LAGs when only one port is receiving protocol transmissions from a partner.

Syntax

set lacp singleportlag {**enable** | **disable**}

Parameters

enable | **disable**	Enables or disables the formation of single port LAGs.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to enable single port LAGs:

```
Matrix(rw)->set lacp singleportlag enable
```

clear singleportlag

Use this command to reset the single port LAG function back to the default state of disabled.

Syntax

clear lacp singleportlag

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to reset the single port LAG function back to disabled:

```
Matrix(rw)->clear lacp singleportlag
```


Downloaded from www.Manualslib.com manuals search engine

show port lacp

Use this command to display link aggregation information for one or more underlying physical ports.

Syntax

show port lacp port *port-string* {[**status** {**detail** | **summary**}] | [**counters**]} [**sort** {**port** | **lag**}]

Parameters

port *port-string*	Displays LACP information for specific port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.
status detail | **summary**	Displays LACP status in detailed or summary information.
counters	Displays LACP counter information.
sort port | **lag**	(Optional) When **summary** is specified, sorts display by port designation or LAG ID.

Defaults

None.

Mode

Switch command, Read-Only.

Examples

This example shows how to display detailed LACP status information for port fe.1.12:

```
Matrix(rw)-> show port lacp port fe.1.12 status detail
Port Instance:               fe.1.12
ActorPort:                      1411  PartnerAdminPort:                    1411
ActorSystemPriority:           32768  PartnerOperPort:                     1411
ActorPortPriority:             32768  PartnerAdminSystemPriority:         32768
ActorAdminKey:                 32768  PartnerOperSystemPriority:          32768
ActorOperKey:                  32768  PartnerAdminPortPriority:           32768
ActorAdminState:             -----GlA  PartnerOperPortPriority:            32768
ActorOperState:              -F----lA  PartnerAdminKey:                     1411
ActorSystemID:    00-e0-63-9d-b5-87  PartnerOperKey:                      1411
SelectedAggID:                  none  PartnerAdminState:               --DCSGlp
AttachedAggID:                  none  PartnerOperState:                --DC-Glp
MuxState:                   Detached  PartnerAdminSystemID:   00-00-00-00-00-00
DebugRxState:          port Disabled  PartnerOperSystemID:    00-00-00-00-00-00
```

Note: State definitions, such as ActorAdminState and Partner AdminState, are indicated with letter abbreviations. If the **show port lacp** command displays one or more of the following letters, it means the state is true for the associated actor or partner ports:
E = Expired; **F** = Defaulted; **D** = Distributing (tx enabled); **C** = Collecting (rx enabled); **S** = Synchronized (actor and partner agree); **G** = Aggregation allowed; **S/I** = Short/Long LACP timeout; **A/p** = Active/Passive LACP.

For more information about these states, refer to **set port lacp** ("set port lacp" on page 4-66) and the IEEE 802.3 2002 specification.

This example shows how to display summarized LACP status information for port fe.1.12:

Downloaded from www.Manualslib.com manuals search engine

```
Matrix(rw)->show port lacp port fe.1.12 status summary
Port     AggrActor System   Partner System
                  Pri:   System ID:  Key:  Pri: System ID:     Key:
fe.1.12    none [(32768,00e0639db587,32768),(32768,000000000000, 1411)]
```

This example shows how to display LACP counters for port fe.1.12:

```
Matrix(rw)->show port lacp port fe.1.12 counters
Port Instance:                          fe.1.12
LACPDUsRx:                           0  MarkerPDUsRX:                          0
LACPDUsTx:                           0  MarkerPDUsTx:                          0
IllegalRx:                           0  MarkerResponsePDUsRx:                  0
UnknownRx:                           0  MarkerResponsePDUsTx:                  0
ActorSyncTransitionCount:            0  PartnerSyncTransitionCount:            0
ActorChangeCount:                    1  PartnerChangeCount:                    0
ActorChurnCount:                     0  PartnerChurnCount:                     0
ActorChurnState:        ChurnMonitor    PartnerChurnState:          ChurnMonitor
MuxState:                   detached
MuxReason:                               BEGIN = TRUE
```

set port lacp

Use this command to set link aggregation parameters for one or more ports.

Syntax

set port lacp port *port-string* {[**aadminkey** *aadminkey*] [**aportpri** *aportpri*] [**asyspri** *asyspri*] [**aadminstate** {**lacpactive** | **lacptimeout** | **lacpagg** | **lacpsync** | **lacpcollect** | **lacpdist** | **lacpdef** | **lacpexpire**}] [**padminsyspri** *padminsyspri*] [**padminsysid** *padminsysid*] [**padminkey** *padminkey*] [**padminportpri** *padminportpri*] [**padminport** *padminport*] [**padminstate** {**lacpactive** | **lacptimeout** | **lacpagg** | **lacpsync** | **lacpcollect** | **lacpdist** | **lacpdef** | **lacpexpire**}] [**enable** | [**disable**]}

Parameters

port *port-string*	Specifies the physical port(s) on which to configure LACP. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.
aadminkey *aadminkey*	Sets the port's actor admin key. LACP will use this value to form an oper key and will determine which underlying physical ports are capable of aggregating by comparing oper keys. Aggregator ports allow only underlying ports with oper keys matching theirs to join their LAG. Valid values are **1** - **65535**.
aportpri *aportpri*	Sets the port's actor port priority. Valid values are **0** - **65535**, with lower values designating higher priority.
asyspri *asyspri*	Sets the port's actor system priority. The LACP implementation on the Matrix Series device uses this value to determine aggregation precedence when there are two devices competing for the same aggregator. Valid values are **0** - **65535**, with higher precedence given to lower values. **Note:** Only one LACP system priority can be set on a Matrix Series device, using either this command, or the **set lacp asyspri** command ("set lacp asyspri" on page 4-60).

Downloaded from www.Manualslib.com manuals search engine

aadminstate lacpactive | lacptimeout | lacpagg | lacpsync | lacpcollect | lacpdist | lacpdef | lacpexpire	Sets the port's actor LACP administrative state to allow for: • **lacpactive -** Transmitting LACP PDUs. • **lacptimeout -** Transmitting LACP PDUs every 1 sec. vs 30 sec. (default). • **lacpagg -** Aggregation on this port. • **lacpsync -** Transition to synchronization state. • **lacpcollect -** Transition to collection state. • **lacpdist -** Transition to distribution state. • **lacpdef** - Transition to defaulted state. • **lacpexpire -** Transition to expired state.
padminsyspri *padminsyspri*	Sets a default value to use as the port's partner priority. Valid values are **0** - **65535**, with lower values given higher priority.
padminsysid *padminsysid*	Sets a default value to use as the port's partner system ID. This is a MAC address.
padminkey *padminkey*	Sets a default value to use as the port's partner admin key. Only ports with matching admin keys are allowed to aggregate. Valid values are **1** - **65535**.
padminportpri *padminportpri*	Sets a default value to use as the port's partner port priority. Valid values are **0** - **65535**, with lower values given higher priority.
padminport *padminport*	Sets a default value to use as the port's partner admin value. Valid values are **1** - **65535**.
padminstate lacpactive | lacptimeout | lacpagg | lacpsync | lacpcollect | lacpdist | lacpdef | lacpexpire	Sets a port's partner LACP administrative state. See **aadminstate** for valid options.
enable	(Optional) Enables LACPDU processing on this port.
disable	(Optional) Disables LACPDU processing on this port.

Defaults

- At least one parameter must be entered per *port-string*.
- If **enable** or **disable** are not specified, port(s) will be enabled with the LACP parameters entered.

Mode

Switch command, Read-Write.

Usage

These settings will determine the specified underlying physical ports' ability to join a LAG, and their administrative state once aggregated.

LACP commands and parameters beginning with an "a" (such as **aadminkey**) set actor values. Corresponding commands and parameters beginning with a "p" (such as **padminkey**) set corresponding partner values. Actor refers to the local device participating in LACP negotiation, while partner refers to its remote device partner at the other end of the negotiation. Actors and

Downloaded from www.Manualslib.com manuals search engine

partners maintain current status of the other via LACPDUs containing information about their ports' LACP status and operational state.

Example

This example shows how to set the actor admin key to 3555 for port ge.3.16:

```
Matrix(rw)->set port lacp ge.3.16 aadminkey 3555
```

clear port lacp

Use this command to clear link aggregation settings for one or more ports.

Syntax

clear port lacp port *port-string* {[**aadminkey**] [**aportpri**] [**asyspri**] [**aadminstate** {**lacpactive** | **lacptimeout** | **lacpagg** | **lacpsync** | **lacpcollect** | **lacpdist** | **lacpdef** | **lacpexpire** | **all**}] [**padminsyspri**] [**padminsysid**] [**padminkey**] [**padminportpri**] [**padminport**] [**padminstate** {**lacpactive** | **lacptimeout** | **lacpagg** | **lacpsync** | **lacpcollect** | **lacpdist** | **lacpdef** | **lacpexpire** | **all**}]}

Parameters

port *port-string*	Specifies the physical port(s) on which LACP settings will be cleared. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.
aadminkey	Clears a port's actor admin key.
aportpri	Clears a port's actor port priority.
asyspri	Clears the port's actor system priority.
aadminstate lacpactive | **lacptimeout** | **lacpagg** | **lacpsync** | **lacpcollect** | **lacpdist** | **lacpdef** | **lacpexpire** | **all**	Clears a port's specific actor admin state, or all actor admin state(s). For descriptions of specific states, refer to the **set port lacp** command ("set port lacp" on page 4-66.)
padminsyspri	Clears the port's default partner priority value.
padminsysid	Clears the port's default partner system ID.
padminkey	Clears the port's default partner admin key.
padminportpri	Clears the port's default partner port priority.
padminport	Deletes a partner port from the LACP configuration.
padminstate lacpactive | **lacptimeout** | **lacpagg** | **lacpsync** | **lacpcollect** | **lacpdist** | **lacpdef** | **lacpexpire** | **all**	Clears the port's specific partner admin state, or all partner admin state(s).

Defaults

None.

Downloaded from www.Manualslib.com manuals search engine

Mode

Switch command, Read-Write.

Example

This example shows how to clear all link aggregation parameters for port ge.3.16:

```
Matrix(rw)->clear port lacp port ge.3.16
```

show lacp flowRegeneration

Use this command to display the LACP flow regeneration state.

Syntax

show lacp flowRegeneration

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Only.

Example

This example shows how to display the current LACP flow regeneration state:

```
Matrix(rw)->show lacp flowRegeneration
disable
```

set lacp flowRegeneration

Use this command to enable or disable LACP flow regeneration.

Syntax

set lacp flowRegeneration {**enable** | **disable**}

Parameters

enable | **disable**	Enables or disables LACP flow regeneration

Defaults

None.

Mode

Switch command, Read-Write.

Downloaded from www.Manualslib.com manuals search engine

Usage

When enabled and a new port joins a link aggregation group (LAG), LACP will redistribute all existing flows over the LAG. It will also attempt to load balance existing flows to take advantage of ports added to the LAG. When flow regeneration is disabled and a new port joins a LAG, LACP will only distribute new flows over the increased number of ports in the LAG and will leave existing flows intact.

Example

This example shows how to enable LACP flow regeneration:

```
Matrix(rw)->set lacp flowRegeneration enable
```

clear lacp flowRegeneration

Use this command to reset LACP flow regeneration to its default state (disabled).

Syntax

clear lacp flowRegeneration

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to reset LACP flow regeneration to disabled:

```
Matrix(rw)->clear lacp flowRegeneration
```

show lacp outportAlgorithm

Use this command to display the current LACP outport algorithm.

Syntax

show lacp outportAlgorithm

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Only.

Downloaded from www.Manualslib.com manuals search engine

Example

This example shows how to display the current LACP:

```
Matrix(rw)->show lacp outportAlgorithmoutport algorithm
dip-sip
```

set lacp outportAlgorithm

Use this command to set the algorithm LACP will use for outport determination.

Syntax

set lacp outportAlgorithm {**dip-sip** | **da-sa** | **round-robin**}

Parameters

dip-sip	Specifies that destination and source IP addresses will determine the LACP outport.
da-sa	Specifies that destination and source MAC addresses will determine the LACP outport.
round-robin	Specifies that the round-robin algorithm will determine the LACP outport.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to set the LACP outport algorithm to DA-SA:

```
Matrix(rw)->set lacp outportalgorithm da-sa
```

clear lacp outportAlgorithm

Use this command to reset LACP to DIP-SIP, its default outport algorithm.

Syntax

clear lacp outportAlgorithm

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Write.

Downloaded from www.Manualslib.com manuals search engine

Example

This example shows how to reset the LACP outport algorithm to DIP-SIP:

```
Matrix(rw)->clear lacp outportAlgorithm
```


Downloaded from www.Manualslib.com manuals search engine

5

SNMP Configuration

This chapter describes the Simple Network Management Protocol (SNMP) set of commands and how to use them.

Note: Commands for configuring SNMP on the Matrix Series device are independent during the SNMP setup process. For instance, target parameters can be specified when setting up optional notification filters — even though these parameters have not yet been created with the **set snmp targetparams** command.

For information about...	Refer to page...
SNMP Configuration Summary	5-1
Reviewing SNMP Statistics	5-5
Configuring SNMP Users, Groups and Communities	5-10
Configuring SNMP Access Rights	5-18
Configuring SNMP MIB Views	5-22
Configuring SNMP Target Parameters	5-26
Configuring SNMP Target Addresses	5-29
Configuring SNMP Notification Parameters	5-33
Configuring SNMP Walk Behavior	5-41

SNMP Configuration Summary

SNMP is an application-layer protocol that facilitates the exchange of management information between network devices. SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth.

Matrix Series devices support three versions of SNMP:

- Version 1 (SNMPv1) — This is the initial implementation of SNMP. Refer to RFC 1157 for a full description of functionality.
- Version 2 (SNMPv2c) — The second release of SNMP, described in RFC 1907, has additions and enhancements to data types, counter size, and protocol operations.
- Version 3 (SNMPv3) — This is the most recent version of SNMP, and includes significant enhancements to administration and security. SNMPv3 is fully described in RFC 2571, RFC 2572, RFC 2573, RFC 2574, and RFC 2575.

Downloaded from www.Manualslib.com manuals search engine

SNMPv1 and SNMPv2c

The components of SNMPv1 and SNMPv2c network management fall into three categories:

- Managed devices (such as a switch)
- SNMP agents and MIBs, including SNMP traps, community strings, and Remote Monitoring (RMON) MIBs, which run on managed devices
- SNMP network management applications, such as Enterasys NetSight, which communicate with agents to get statistics and alerts from the managed devices.

SNMPv3

SNMPv3 is an interoperable standards-based protocol that provides secure access to devices by authenticating and encrypting frames over the network. The advanced security features provided in SNMPv3 are as follows:

- Message integrity — Collects data securely without being tampered with or corrupted.
- Authentication — Determines the message is from a valid source.
- Encryption — Scrambles the contents of a frame to prevent it from being seen by an unauthorized source.

Unlike SNMPv1 and SNMPv2c, in SNMPv3, the concept of SNMP agents and SNMP managers no longer apply. These concepts have been combined into an SNMP entity. An SNMP entity consists of an SNMP engine and SNMP applications. An SNMP engine consists of the following four components:

- Dispatcher — This component sends and receives messages.
- Message processing subsystem — This component accepts outgoing PDUs from the dispatcher and prepares them for transmission by wrapping them in a message header and returning them to the dispatcher. The message processing subsystem also accepts incoming messages from the dispatcher, processes each message header, and returns the enclosed PDU to the dispatcher.
- Security subsystem — This component authenticates and encrypts messages.
- Access control subsystem — This component determines which users and which operations are allowed access to managed objects.

About SNMP Security Models and Levels

An SNMP security model is an authentication strategy that is set up for a user and the group in which the user resides. A security level is the permitted level of security within a security model. The three levels of SNMP security are: No authentication required (NoAuthNoPriv); authentication required (AuthNoPriv); and privacy (authPriv). A combination of a security model and a security level determines which security mechanism is employed when handling an SNMP frame. Table 5-1 identifies the levels of SNMP security available on Matrix Series devices and authentication required within each model.

Downloaded from www.Manualslib.com manuals search engine

Table 5-1 SNMP Security Levels

Model	Security Level	Authentication	Encryption	How It Works
v1	NoAuthNoPriv	Community string	None	Uses a community string match for authentication.
v2c	NoAuthNoPriv	Community string	None	Uses a community string match for authentication.
v3	NoAuthNoPriv	User name	None	Uses a user name match for authentication.
	AuthNoPriv	MD5 or SHA	None	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms.
	authPriv	MD5 or SHA	DES	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. Provides DES 56-bit encryption in addition to authentication based on the CBC-DES (DES-56) standard.

Using SNMP Contexts to Access Specific MIBs

By default, when operating from the switch CLI, Matrix Series devices allow access to all SNMP MIBs or contexts. A context is a collection of MIB objects, often associated with a particular physical or logical device.

If no optional *context* parameters are configured for v1 and v2 "community" names and v3 "user" groups, these groups are able to access all SNMP MIB objects when in switch mode.

Specifying a *context* parameter when setting up SNMP user group access would permit or restrict the group's switch management access to the MIB(s) specified by the *context* (MIB object ID) value.

All SNMP contexts known to the device can be displayed using the **show snmp context** command as described in "show snmp context" on page 5-23.

Examples

This example permits the "powergroup" to manage all MIBs via SNMPv3:

```
Matrix(rw)->set snmp access powergroup security-model usm
```

This example grants the "powergroup" SNMPv3 management access from the module operating in router mode:

```
Matrix(rw)->set snmp access powergroup security-model usm context router prefix
```

For information on preparing the device for router mode, refer back to "Preparing the Device for Router Mode" on page 2-100.

Creating a Basic SNMP Trap Configuration

Traps are notification messages sent by an SNMPv1 or v2 agent to a network management station, a console, or a terminal to indicate the occurrence of a significant event, such as when a port or device goes up or down, when there are authentication failures, and when power supply errors occur. The following configuration example shows how to use CLI commands to associate SNMP notification parameters with security and authorization criteria (target parameters), and map the parameters to a management target address.

Downloaded from www.Manualslib.com manuals search engine

Note: This example illustrates how to configure an SNMPv2 trap notification. Creating an SNMPv1 or v3 Trap, or an SNMPv3 Inform notification would require using the same commands with different parameters, where appropriate. Always ensure that v1/v2 communities or v3 users used for generating traps or informs are pre-configured with enough privileges to access corresponding MIBs.

Complete an SNMPv2 trap configuration on a Matrix Series device as follows:

1. Create a community name that will act as an SNMP user password.
2. Create an SNMP target parameters entry to associate security and authorization criteria to the users in the community created in Step 1.
3. Verify if any applicable SNMP notification entries exist, or create a new one. You will use this entry to send SNMP notification messages to the appropriate management targets created in Step 2.
4. Create a target address entry to bind a management IP address to:
   - The notification entry and tag name created in Step 3.
   - The target parameters entry created in Step 2.

Table 5-2 shows the commands used to complete an SNMPv2 trap configuration on a Matrix Series device.

Table 5-2 Basic SNMP Trap Configuration Command Set

To do this...	Use these commands...
Create a community name.	**set snmp community (**“set snmp community” on page 5-16**)**
Create an SNMP target parameters entry.	**set snmp targetparams (**“set snmp targetparams” on page 5-27**)**
Verify if any applicable SNMP notification entries exist.	**show snmp notify** (“show snmp notify” on page 5-33)
Create a new notification entry.	**set snmp notify (**“set snmp notify” on page 5-35**)**
Create a target address entry.	set snmp targetaddr (“set snmp targetaddr” on page 5-30)

Example

This example shows how to:

- create an SNMP community called **mgmt**
- configure a trap notification called **TrapSink**
  This trap notification will be sent with the community name **mgmt** to the workstation **192.168.190.80** (which is target address **tr**). It will use security and authorization criteria contained in a target parameters entry called **v2cExampleParams**.

```
Matrix(rw)->set snmp community mgmt
Matrix(rw)->set snmp targetparams v2cExampleParams user mgmt
security-model v2c message-processing v2c
Matrix(rw)->set snmp notify entry1 tag TrapSink
Matrix(rw)->set snmp targetaddr tr 192.168.190.80 param v2cExampleParams taglist
TrapSink
```


Downloaded from www.Manualslib.com manuals search engine

How SNMP Will Use This Configuration

In order to send a trap/notification requested by a MIB code, the SNMP agent requires the equivalent of a trap "door", a "key" to unlock the door, and a "procedure" for crossing the doorstep. To determine if all these elements are in place, the SNMP agent proceeds as follows:

1. Determines if the "keys" for trap "doors" do exist. In the example configuration above, the key that SNMP is looking for is the notification entry created with the **set snmp notify** command which, in this case, is a key labeled **entry1**.
2. Searches for the doors matching such a key. For example, the parameters set for the **entry1** key shows that it opens only the door **TrapSink**.
3. Verifies that the specified door **TrapSink** is, in fact, available. In this case it was built using the **set snmp targetaddr** command. This command also specifies that this door leads to the management station **192.168.190.80**, and the "procedure" (**targetparams**) to cross the doorstep is called **v2ExampleParams**.
4. Verifies that the **v2ExampleParams** description of how to step through the door is, in fact, there. The agent checks **targetparams** entries and determines this description was made with the **set snmp targetparams** command, which tells exactly which SNMP protocol to use and what community name to provide. In this case, the community name is **mgmt**.
5. Verifies that the **mgmt** community name is available. In this case, it has been configured using the **set snmp community** command.
6. Sends the trap notification message.

Reviewing SNMP Statistics

Purpose

To review SNMP statistics.

Commands

For information about...	Refer to page...
show snmp engineid	5-5
show snmp counters	5-6

show snmp engineid

Use this command to display the SNMP local engine ID. This is the SNMP v3 engine's administratively unique identifier.

Syntax

```
show snmp engineid
```

Parameters

None.

Downloaded from www.Manualslib.com manuals search engine

Defaults

None.

Mode

Switch command, Read-Only.

Example

This example shows how to display SNMP engine properties:

```
Matrix(rw)->show snmp engineid
EngineId: 80:00:15:f8:03:00:e0:63:9d:b5:87
Engine Boots    = 12
Engine Time     = 162181
Max Msg Size    = 2048
```

Table 5-3 shows a detailed explanation of the command output.

Table 5-3 show snmp engineid Output Details

Output...	What it displays...
EngineId	String identifying the SNMP agent on the device.
Engine Boots	Number of times the SNMP engine has been started or reinitialized.
Engine Time	Time in seconds since last reboot.
Max Msg Size	Maximum accepted length, in bytes, of SNMP frame.

show snmp counters

Use this command to display SNMP traffic counter values.

Syntax

show snmp counters

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Only.

Example

This example shows how to display SNMP counter values.

```
Matrix(rw)->show snmp counters

--- mib2 SNMP group counters:
snmpInPkts              = 396601
```


Downloaded from www.Manualslib.com manuals search engine

```
snmpOutPkts             = 396601
snmpInBadVersions       = 0
snmpInBadCommunityNames = 0
snmpInBadCommunityUses  = 0
snmpInASNParseErrs      = 0
snmpInTooBigs           = 0
snmpInNoSuchNames       = 0
snmpInBadValues         = 0
snmpInReadOnlys         = 0
snmpInGenErrs           = 0
snmpInTotalReqVars      = 403661
snmpInTotalSetVars      = 534
snmpInGetRequests       = 290
snmpInGetNexts          = 396279
snmpInSetRequests       = 32
snmpInGetResponses      = 0
snmpInTraps             = 0
snmpOutTooBigs          = 0
snmpOutNoSuchNames      = 11
```

Table 5-4 shows a detailed explanation of the command output.

Table 5-4 show snmp counters Output Details

Output...	What it displays...
snmpInPkts	Number of messages delivered to the SNMP entity from the transport service.
snmpOutPkts	Number of SNMP messages passed from the SNMP protocol entity to the transport service.
snmpInBadVersions	Number of SNMP messages delivered to the SNMP entity for an unsupported SNMP version.
snmpInBadCommunityNames	Number of SNMP messages delivered to the SNMP entity that used an SNMP community name not known to the entity.
snmpInBadCommunityUses	Number of SNMP messages delivered to the SNMP entity that represented an SNMP operation not allowed by the SNMP community named in the message.
snmpInASNParseErrs	Number of ASN.1 (Abstract Syntax Notation) or BER (Basic Encoding Rules) errors encountered by the SNMP entity when decoding received SNMP messages.
snmpInTooBigs	Number of SNMP PDUs delivered to the SNMP protocol entity with the value of the error-status field as “tooBig.”
snmpInNoSuchNames	Number of SNMP PDUs delivered to the SNMP protocol entity with the value of the error-status field as “noSuchName.”
snmpInBadValues	Number of SNMP PDUs delivered to the SNMP protocol entity with the value of the error-status field as “badValue.”
snmpInReadOnlys	Number of valid SNMP PDUs delivered to the SNMP protocol entity with the value of the error-status field as “readOnly.”

Downloaded from www.Manualslib.com manuals search engine

Table 5-4 show snmp counters Output Details (continued)

Output...	What it displays...
snmpInGenErrs	Number of SNMP PDUs delivered to the SNMP protocol entity with the value of the error-status field as “genErr.”
snmpInTotalReqVars	Number of MIB objects retrieved successfully by the SNMP protocol entity as the result of receiving valid SNMP Get-Request and Get-Next PDUs.
snmpInTotalSetVars	Number of MIB objects altered successfully by the SNMP protocol entity as the result of receiving valid SNMP Set-Request PDUs.
snmpInGetRequests	Number of SNMP Get-Request PDUs accepted and processed by the SNMP protocol entity.
snmpInGetNexts	Number of SNMP Get-Next PDUs accepted and processed by the SNMP protocol entity.
snmpInSetRequests	Number of SNMP Set-Request PDUs accepted and processed by the SNMP protocol entity.
snmpInGetResponses	Number of SNMP Get-Response PDUs accepted and processed by the SNMP protocol entity.
snmpInTraps	Number of SNMP Trap PDUs accepted and processed by the SNMP protocol entity.
snmpOutTooBigs	Number of SNMP PDUs generated by the SNMP protocol entity with the value of the error-status field as “tooBig.”
snmpOutNoSuchNames	Number of SNMP PDUs generated by the SNMP protocol entity with the value of the error-status as “noSuchName.”
snmpOutBadValues	Number of SNMP PDUs generated by the SNMP protocol entity with the value of the error-status field as “badValue.”
snmpOutGenErrs	Number of SNMP PDUs generated by the SNMP protocol entity with the value of the error-status field as “genErr.”
snmpOutGetRequests	Number of SNMP Get-Request PDUs generated by the SNMP protocol entity.
snmpOutGetNexts	Number of SNMP Get-Next PDUs generated by the SNMP protocol entity.
snmpOutSetRequests	Number of SNMP Set-Request PDUs generated by the SNMP protocol entity.
snmpOutGetResponses	Number of SNMP Get-Response PDUs generated by the SNMP protocol entity.
snmpOutTraps	Number of SNMP Trap PDUs generated by the SNMP protocol entity.
snmpSilentDrops	Number of SNMP Get, Set, or Inform request error messages that were dropped because the reply was larger than the requestor’s maximum message size.
snmpProxyDrops	Number of SNMP Get, Set, or Inform request error messages that were dropped because the reply was larger than the proxy target’s maximum message size.
usmStatsUnsupportedSecLevels	Number of packets received by the SNMP engine that were dropped because they requested a security level that was unknown to the SNMP engine or otherwise unavailable.

Downloaded from www.Manualslib.com manuals search engine

Table 5-4 show snmp counters Output Details (continued)

Output...	What it displays...
usmStatsNotInTimeWindows	Number of packets received by the SNMP engine that were dropped because they appeared outside of the authoritative SNMP engine's window.
usmStatsUnknownUserNames	Number of packets received by the SNMP engine that were dropped because they referenced a user that was not known to the SNMP engine.
usmStatsUnknownEngineIDs	Number of packets received by the SNMP engine that were dropped because they referenced an snmpEngineID that was not known to the SNMP engine.
usmStatsWrongDigests	Number of packets received by the SNMP engine that were dropped because they did not contain the expected digest value.
usmStatsDecriptionErrors	Number of packets received by the SNMP engine that were dropped because they could not be decrypted.

Downloaded from www.Manualslib.com manuals search engine

Configuring SNMP Users, Groups and Communities

Purpose

To review and configure SNMP users, groups and v1 and v2 communities. These are defined as follows:

- User — A person registered in SNMPv3 to access SNMP management.
- Group — A collection of users who share the same SNMP access privileges.
- Community — A name used to authenticate SNMPv1 and v2 users.

Commands

For information about...	Refer to page...
show snmp user	5-10
set snmp user	5-12
clear snmp user	5-12
show snmp group	5-13
set snmp group	5-14
clear snmp group	5-15
show snmp community	5-15
set snmp community	5-16
clear snmp community	5-17

show snmp user

Use this command to display information about SNMP users. These are people registered to access SNMP management.

Syntax

show snmp user [**list**] | [*user*] | [**remote** *remote*] [**volatile** | **nonvolatile** | **read-only**]

Parameters

list	(Optional) Displays a list of registered SNMP user names.
user	(Optional) Displays information about a specific user.
remote *remote*	(Optional) Displays information about users on a specific remote SNMP engine.
volatile | **nonvolatile** | **read-only**	(Optional) Displays user information for a specified storage type.

Defaults

- If **list** is not specified, detailed SNMP information will be displayed.

Downloaded from www.Manualslib.com manuals search engine

- If *user* is not specified, information about all SNMP users will be displayed.
- If **remote** is not specified, user information about the local SNMP engine will be displayed.
- If not specified, user information for all storage types will be displayed.

Mode

Switch command, Read-Only.

Examples

This example shows how to display an SNMP user list:

```
Matrix(rw)->show snmp user list
--- SNMP user information ---
--- List of registered users:
Guest
admin1
admin2
netops
```

This example shows how to display information for the SNMP "guest" user:

```
Matrix(rw)->show snmp user guest
--- SNMP user information ---
EngineId:  00:00:00:63:00:00:00:a1:00:00:00:00
Username                = Guest
Auth protocol           = usmNoAuthProtocol
Privacy protocol        = usmNoPrivProtocol
Storage type            = nonVolatile
Row status              = active
```

Table 5-5 shows a detailed explanation of the command output.

Table 5-5 show snmp user Output Details

Output...	What it displays...
EngineId	SNMP local engine identifier.
Username	SNMPv1 or v2 community name or SNMPv3 user name.
Auth protocol	Type of authentication protocol applied to this user.
Privacy protocol	Whether a privacy protocol is applied when authentication protocol is in use.
Storage type	Whether entry is stored in **volatile**, **nonvolatile**, or **read-only** memory.
Row status	Status of this entry: **active**, **notInService**, or **notReady**.

Downloaded from www.Manualslib.com manuals search engine

set snmp user

Use this command to create a new SNMPv3 user.

Syntax

set snmp user *user* [**remote** *remoteid*] [**authentication** {**md5** | **sha**}] [*authpassword*] [**privacy** *privpassword*] [**volatile** | **nonvolatile**]

Parameters

user	Specifies a name for the SNMPv3 user.
remote *remoteid*	(Optional) Registers the user on a specific remote SNMP engine.
authentication md5 | **sha**	(Optional) Specifies the authentication type required for this user as MD5 or SHA.
authpassword	(Optional) Specifies a password for this user when authentication is required. Minimum of 8 characters.
privacy *privpassword*	(Optional) Applies encryption and specifies an encryption password. Minimum of 8 characters
volatile | **nonvolatile**	(Optional) Specifies a storage type for this user entry.

Defaults

- If **remote** is not specified, the user will be registered for the local SNMP engine.
- If **authentication** is not specified, no authentication will be applied.
- If **privacy** is not specified, no encryption will be applied.
- If storage type is not specified, **nonvolatile** will be applied.

Mode

Switch command, Read-Write.

Example

This example shows how to create a new SNMP user named "netops". By default, this user will be registered on the local SNMP engine without authentication and encryption. Entries related to this user will be stored in permanent (nonvolatile) memory:

```
Matrix(rw)->set snmp user netops
```

clear snmp user

Use this command to remove a user from the SNMPv3 security-model list.

Syntax

clear snmp user *user* [**remote** *remote*]

Parameters

user	Specifies an SNMPv3 user to remove.
remote *remote*	(Optional) Removes the user from a specific remote SNMP engine.

Downloaded from www.Manualslib.com manuals search engine

Defaults

If **remote** is not specified, the user will be removed from the local SNMP engine.

Mode

Switch command, Read-Write.

Example

This example shows how to remove the SNMP user named "bill":

```
Matrix(rw)->clear snmp user bill
```

show snmp group

Use this command to display an SNMP group configuration. An SNMP group is a collection of SNMPv3 users who share the same access privileges.

Syntax

show snmp group [**groupname** *groupname*] [**user** *user*] [**security-model** {**v1** | **v2c** | **usm**}] [**volatile** | **nonvolatile** | **read-only**]

Parameters

groupname *groupname*	(Optional) Displays information for a specific SNMP group.
user *user*	(Optional) Displays information about users within the specified group.
security-model v1 | **v2c** | **usm**	(Optional) Displays information about groups assigned to a specific security SNMP model.
volatile | **nonvolatile** | **read-only**	(Optional) Displays SNMP group information for a specified storage type.

Defaults

- If *groupname* is not specified, information about all SNMP groups will be displayed.
- If *user* is not specified, information about all SNMP users will be displayed.
- If **security-model** is not specified, user information about all SNMP versions will be displayed.
- If not specified, information for all storage types will be displayed.

Mode

Switch command, Read-Only.

Example

This example shows how to display SNMP group information:

```
Matrix(rw)->show snmp group
--- SNMP group information ---
Security model          = SNMPv1
Security/user name      = public
Group name              = Anyone
```


Downloaded from www.Manualslib.com manuals search engine

```
Storage type            = nonVolatile
Row status              = active

Security model          = SNMPv1
Security/user name      = public.router
Group name              = Anyone
Storage type            = nonVolatile
Row status              = active
```

Table 5-6 shows a detailed explanation of the command output.

Table 5-6 show snmp group Output Details

Output...	What it displays...
Security model	SNMP version associated with this group.
Security/user name	User belonging to the SNMP group.
Group name	Name of SNMP group.
Storage type	Whether entry is stored in **volatile**, **nonvolatile** or **read-only** memory.
Row status	Status of this entry: **active**, **notInService,** or **notReady**.

set snmp group

Use this command to create an SNMP group. This associates SNMPv3 users to a group that shares common access privileges.

Syntax

set snmp group *groupname* **user** *user* **security-model** {**v1** | **v2c** | **usm**} [**volatile** | **nonvolatile**]

Parameters

groupname	Specifies an SNMP group name to create.
user *user*	Specifies an SNMPv3 user name to assign to the group.
security-model v1 | **v2c** | **usm**	Specifies an SNMP security model to assign to the group.
volatile | **nonvolatile**	(Optional) Specifies a storage type for SNMP entries associated with the group.

Defaults

If storage type is not specified, **nonvolatile** storage will be applied.

Mode

Switch command, Read-Write.

Downloaded from www.Manualslib.com manuals search engine

Example

This example shows how to create an SNMP group called “anyone”, assign a user named “public” and assign SNMPv3 security to the group:

```
Matrix(rw)->set snmp group anyone user public security-model usm
```

clear snmp group

Use this command to clear SNMP group settings globally or for a specific SNMP group and user.

Syntax

clear snmp group *groupname user* [**security-model** {**v1** | **v2c** | **usm**}]

Parameters

groupname	Specifies the SNMP group to be cleared.
user	Specifies the SNMP user to be cleared.
security-model v1 | **v2c** | **usm**	(Optional) Clears the settings associated with a specific security model.

Defaults

If not specified, settings related to all security models will be cleared.

Mode

Switch command, Read-Write.

Example

This example shows how to clear all settings assigned to the “public” user within the SNMP group “anyone”:

```
Matrix(rw)->clear snmp group anyone public
```

show snmp community

Use this command to display SNMP community names and status. In SNMPv1 and v2, community names act as passwords to remote management.

Syntax

```
show snmp community [name]
```

Parameters

name	(Optional) Displays SNMP information for a specific community name.

Defaults

If *name* is not specified, information will be displayed for all SNMP communities.

Mode

Switch command, Read-Only.

Downloaded from www.Manualslib.com manuals search engine

Example

This example shows how to display information about the SNMP "public" community name. For a description of this output, refer to "set snmp community" on page 5-16:

```
Matrix(rw)->show snmp community public

--- Configured community strings ---

Name            = public
Security name   = public
Context         =
Transport tag   =
Storage type    = nonVolatile
Status          = active
```

set snmp community

Use this command to configure an SNMP community group.

Syntax

set snmp community *community* [**securityname** *securityname*] [**context** *context*] [**transport** *transport*] [**volatile** | **nonvolatile**]

Parameters

community	Specifies a community group name.
securityname *securityname*	(Optional) Specifies an SNMP security name to associate with this community. Default: If no security name is specified, the community name is used.
context *context*	(Optional) Specifies a subset of management information this community will be allowed to access. Valid values are full or partial context names of either MIB object IDs or **router** (the system designated router mode module). Default: All MIB objects. To review all contexts configured for the device, use the **show snmp context** command as described in "show snmp context" on page 5-23. **Note:** Beginning with Release 6.0 do not specify the routing module ID as part of the *context*. You must specify **router** for the system designated router mode module.
transport *transport*	(Optional) Specifies the set of transport endpoints from which SNMP request with this community name will be accepted. Makes a link to a target address table. Default: None.
volatile | **nonvolatile**	(Optional) Specifies the storage type for these entries. Default: nonvolatile.

Defaults

None.

Mode

Switch command, Read-Write.

Downloaded from www.Manualslib.com manuals search engine

Examples

This example shows how to set an SNMP community name called “vip”:

```
Matrix(rw)->set snmp community vip
```

This example shows how to grant SNMP management privileges to “vip” community from the routing module operating in router mode:

```
Matrix(rw)->set snmp community vip context router
```

clear snmp community

Use this command to delete an SNMP community name.

Syntax

clear snmp community *name*

Parameters

name	Specifies the SNMP community name to clear.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to delete the community name “vip.”

```
Matrix(rw)->clear snmp community vip
```


Downloaded from www.Manualslib.com manuals search engine

Configuring SNMP Access Rights

Purpose

To review and configure SNMP access rights and assign viewing privileges and security levels to SNMP user groups.

Commands

For information about...	Refer to page...
show snmp access	5-18
set snmp access	5-20
clear snmp access	5-21
set snmp timefilter break	5-41

show snmp access

Use this command to display access rights and security levels configured for SNMP one or more groups.

Syntax

show snmp access [*groupname*] [**security-model** {**v1** | **v2c** | **usm**}] [**noauthentication** | **authentication** | **privacy**] [**context** *context*] [**volatile** | **nonvolatile** | **read-only**]

Parameters

groupname	(Optional) Displays access information for a specific SNMPv3 group.
security-model v1 | **v2c** | **usm**	(Optional) Displays access information for SNMP security model version 1, 2c or 3 (usm).
noauthentication | **authentication** | **privacy**	(Optional) Displays access information for a specific security level.
context *context*	(Optional) Displays access information for a specific context. For a description of how to specify SNMP contexts, refer to "Using SNMP Contexts to Access Specific MIBs" on page 5-3.
volatile | **nonvolatile** | **read-only**	(Optional) Displays access entries for a specific storage type.

Defaults

- If *groupname* is not specified, access information for all SNMP groups will be displayed.
- If **security-model** is not specified, access information for all SNMP versions will be displayed.
- If **noauthentication**, **authentication** or **privacy** are not specified, access information for all security levels will be displayed.
- If **context** is not specified, all contexts will be displayed.

Downloaded from www.Manualslib.com manuals search engine

- If **volatile**, **nonvolatile** or **read-only** are not specified, all entries of all storage types will be displayed.

Mode

Switch command, Read-Only.

Example

This example shows how to display SNMP access information:

```
Matrix(rw)->show snmp access
Group           = SystemAdmin
Security model  = USM
Security level  = noAuthNoPriv
Read View       = All
Write View      =
Notify View     = All
Context match   = exact match
Storage type    = nonVolatile
Row status      = active

Group           = NightOperator
Security model  = USM
Security level  = noAuthNoPriv
Read View       = All
Write View      =
Notify View     = All
Context match   = exact match
Storage type    = nonVolatile
Row status      = active
```

Table 5-7 shows a detailed explanation of the command output.

Table 5-7 show snmp access Output Details

Output...	What it displays...
Group	SNMP group name.
Security model	Security model applied to this group. Valid types are: **SNMPv1**, **SNMPv2c**, and SNMPv3 (User based - **USM**).
Security level	Security level applied to this group. Valid levels are: • noAuthNoPrivacy (**no authentication** required) • AuthNoPrivacy (**authentication** required) • authPriv (**privacy** -- most secure level)
Read View	Name of the view that allows this group to view SNMP MIB objects.
Write View	Name of the view that allows this group to configure the contents of the SNMP agent.
Notify View	Name of the view that allows this group to send an SNMP trap message.

Downloaded from www.Manualslib.com manuals search engine

Table 5-7 show snmp access Output Details (continued)

Output...	What it displays...
Context match	Whether or not SNMP context match must be exact (full context name match) or a partial match with a given prefix.
Storage type	Whether access entries for this group are stored in **volatile**, **nonvolatile** or **read-only** memory.
Row status	Status of this entry: **active**, **notInService**, or **notReady**.

set snmp access

Use this command to set an SNMP access configuration.

Syntax

set snmp access *groupname* **security-model** {**v1** | **v2c** | **usm**} [**noauthentication** | **authentication** | **privacy**] [**context** *context*] [**exact** | **prefix**] [**read** *read*] [**write** *write*] [**notify** *notify*] [**volatile** | **nonvolatile**]

Parameters

groupname	Specifies a name for an SNMPv3 group.
security-model v1 | **v2c** | **usm**	Specifies SNMP version 1, 2c or 3 (usm).
noauthentication | **authentication** | **privacy**	(Optional) Applies SNMP security level as no authentication, authentication (without privacy) or privacy. Privacy specifies that messages sent on behalf of the user are protected from disclosure.
context *context* **exact** | **prefix**	(Optional) Sets the context for this access configuration and specifies that the match must be exact (matching the whole context string) or a prefix match only. Context is a subset of management information this SNMP group will be allowed to access. Valid values are full or partial MIB object context names and **router** for the module operating in router mode. To review all contexts configured for the device, use the **show snmp context** command as described in "show snmp context" on page 5-23. **Note:** Beginning with Release 6.0, do not specify the routing module ID as part of the *context*. You must specify **router** for the system designated router mode module.
read *read*	(Optional) Specifies a read access view.
write *write*	(Optional) Specifies a write access view.
notify *notify*	(Optional) Specifies a notify access view.
volatile | **nonvolatile** | **read-only**	(Optional) Stores associated SNMP entries as temporary or permanent, or read-only.

Defaults

- If security level is not specified, no authentication will be applied.
- If **context** is not specified, access will be enabled for the default context. If **context** is specified without a context match, **exact** match will be applied.
- If **read** view is not specified none will be applied.

Downloaded from www.Manualslib.com manuals search engine

- If **write** view is not specified, none will be applied.
- If **notify** view is not specified, none will be applied.
- If storage type is not specified, entries will be stored as permanent and will be held through device reboot.

Mode

Switch command, Read-Write.

Examples

This example permits the "powergroup" to manage all MIBs via SNMPv3:

```
Matrix(rw)->set snmp access powergroup security-model usm
```

This example grants the "powergroup" SNMPv3 management access from all router modules when operating in router mode:

```
Matrix(rw)->set snmp access powergroup security-model usm context router prefix
```

clear snmp access

Use this command to clear the SNMP access entry of a specific group, including its set SNMP security-model, and level of security.

Syntax

clear snmp access *groupname* **security-model** {**v1** | **v2c** | **usm**} [**noauthentication** | **authentication** | **privacy**] [**context** *context*]

Parameters

groupname	Specifies the name of the SNMP group for which to clear access.
security-model v1 | **v2c** | **usm**	Specifies the security model to be cleared for the SNMP access group.
noauthentication | **authentication** | **privacy**	(Optional) Clears a specific security level for the SNMP access group.
context *context*	(Optional) Clears a specific context for the SNMP access group. Enter / - / to clear the default context.

Defaults

- If security level is not specified, all levels will be cleared.
- If **context** is not specified, none will be applied.

Mode

Switch command, Read-Write.

Example

This example shows how to clear SNMP version 3 access for the "mis-group" via the authentication protocol:

```
Matrix(rw)->clear snmp access mis-group security-model usm authentication
```


Downloaded from www.Manualslib.com manuals search engine

Configuring SNMP MIB Views

Purpose

To review and configure SNMP MIB views. SNMP views map SNMP objects to access rights.

Commands

For information about...	Refer to page...
show snmp view	5-22
show snmp context	5-23
set snmp view	5-24
clear snmp view	5-25

show snmp view

Use this command to display the MIB configuration for SNMPv3 view-based access (VACM).

Syntax

show snmp view [*viewname*] [**subtree** *oid-or-mibobject*] [**volatile** | **nonvolatile** | **read-only**]

Parameters

viewname	(Optional) Displays information for a specific MIB view.
subtree *oid-or-mibobject*	(Optional) Displays information for a specific MIB subtree when *viewname* is specified.
volatile | **nonvolatile** | **read-only**	(Optional) Displays entries for a specific storage type.

Defaults

If no parameters are specified, all SNMP MIB view configuration information will be displayed.

Mode

Switch command, Read-Only.

Example

This example shows how to display SNMP MIB view configuration information:

```
Matrix(rw)->show snmp view

 --- SNMP MIB View information ---
View Name       = All
Subtree OID     = 1
Subtree mask    =
```


Downloaded from www.Manualslib.com manuals search engine

```
View Type       = included
Storage type    = nonVolatile
Row status      = active

View Name       = All
Subtree OID     = 0.0
Subtree mask    =
View Type       = included
Storage type    = nonVolatile
Row status      = active

View Name       = Network
Subtree OID     = 1.3.6.1.2.1
Subtree mask    =
View Type       = included
Storage type    = nonVolatile
Row status      = active
```

Table 5-8 provides an explanation of the command output. For details on using the **set snmp view** command to assign variables, refer to "set snmp view" on page 5-24.

Table 5-8 show snmp view Output Details

Output...	What it displays...
View Name	Name assigned to a MIB view.
Subtree OID	Name identifying a MIB subtree.
Subtree mask	Bitmask applied to a MIB subtree.
View Type	Whether or not subtree use must be **included** or **excluded** for this view.
Storage type	Whether storage is in **nonVolatile** or **Volatile** memory
Row status	Status of this entry: **active**, **notInService**, or **notReady**.

show snmp context

Use this command to display the context list configuration for SNMP's view-based access control.

Syntax

show snmp context

Parameters

None.

Defaults

None.

Downloaded from www.Manualslib.com manuals search engine

Mode

Switch command, Read-Only.

Usage

An SNMP context is a collection of management information that can be accessed by an SNMP agent or entity. The default context allows all SNMP agents to access all management information (MIBs). When created using the **set snmp access** command ("set snmp access" on page 5-20), other contexts can be applied to limit access to a subset of management information and to permit SNMP access from one or more routing modules.

Example

This example shows how to display a list of all SNMP contexts known to the device:

```
Matrix(rw)->show snmp context

--- Configured contexts:
default context (all mibs)
router
```

set snmp view

Use this command to set a MIB configuration for SNMPv3 view-based access (VACM).

Syntax

set snmp view viewname *viewname* **subtree** *subtree* [**mask** *mask*] [**included** | **excluded**] [**volatile** | **nonvolatile**]

Parameters

viewname *viewname*	Specifies a name for a MIB view.
subtree *subtree*	Specifies a MIB subtree name.
mask *mask*	(Optional) Specifies a bitmask for a subtree.
included | **excluded**	(Optional) Specifies subtree use (default) or no subtree use.
volatile | **nonvolatile**	(Optional) Specifies the use of temporary or permanent (default) storage.

Defaults

- If not specified, **mask** will be set to **255.255.255.255**
- If not specified, subtree use will be **included**.
- If storage type is not specified, **nonvolatile** (permanent) will be applied.

Mode

Switch command, Read-Write.

Downloaded from www.Manualslib.com manuals search engine

Example

This example shows how to set an SNMP MIB view to “public” with a subtree name of 1.3.6.1 included:

```
Matrix(rw)->set snmp view viewname public subtree 1.3.6.1 included
```

clear snmp view

Use this command to delete an SNMPv3 MIB view.

Syntax

clear snmp view *viewname subtree*

Parameters

viewname	Specifies the MIB view name to be deleted.
subtree	Specifies the subtree name of the MIB view to be deleted.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to delete SNMP MIB view “public”:

```
Matrix(rw)->clear snmp view public 1.3.6.1
```


Downloaded from www.Manualslib.com manuals search engine

Configuring SNMP Target Parameters

Purpose

To review and configure SNMP target parameters. This controls where and under what circumstances SNMP notifications will be sent. A target parameter entry can be bound to a target IP address allowed to receive SNMP notification messages with the **set snmp targetaddr** command ("set snmp targetaddr" on page 5-30)

Commands

For information about...	Refer to page...
show snmp targetparams	5-26
set snmp targetparams	5-27
clear snmp targetparams	5-28

show snmp targetparams

Use this command to display SNMP parameters used to generate a message to a target.

Syntax

show snmp targetparams [*targetParams*] [**volatile** | **nonvolatile** | **read-only**]

Parameters

targetParams	(Optional) Displays entries for a specific target parameter.
volatile | **nonvolatile** | **read-only**	(Optional) Displays target parameter entries for a specific storage type.

Defaults

- If *targetParams* is not specified, entries associated with all target parameters will be displayed.
- If not specified, entries of all storage types will be displayed.

Mode

Switch command, Read-Only.

Example

This example shows how to display SNMP target parameters information:

```
Matrix(rw)->show snmp targetparams

--- SNMP TargetParams information ---
Target Parameter Name   = v1ExampleParams
Security Name           = public
Message Proc. Model     = SNMPv1
Security Level          = noAuthNoPriv
```


Downloaded from www.Manualslib.com manuals search engine

```
Storage type            = nonVolatile
Row status              = active

Target Parameter Name   = v2cExampleParams
Security Name           = public
Message Proc. Model     = SNMPv2c
Security Level          = noAuthNoPriv
Storage type            = nonVolatile
Row status              = active

Target Parameter Name   = v3ExampleParams
Security Name           = CharlieDChief
Message Proc. Model     = USM
Security Level          = authNoPriv
Storage type            = nonVolatile
Row status              = active
```

Table 5-9 shows a detailed explanation of the command output.

Table 5-9 show snmp targetparams Output Details

Output...	What it displays...
Target Parameter Name	Unique identifier for the parameter in the SNMP target parameters table. Maximum length is 32 bytes.
Security Name	Security string definition.
Message Proc. Model	SNMP version.
Security Level	Type of security level (**auth**: security level is set to use authentication protocol, **noauth**: security level is not set to use authentication protocol, or **privacy**).
Storage type	Whether entry is stored in **volatile**, **nonvolatile**, or **read-only** memory.
Row status	Status of this entry: **active**, **notInService**, or **notReady**.

set snmp targetparams

Use this command to set SNMP target parameters, a named set of security/authorization criteria used to generate a message to a target.

Syntax

set snmp targetparams *paramsname* **user** *user* **security-model** {**v1** | **v2c** | **usm**} **message-processing** {**v1** | **v2c** | **v3**} [**noauthentication** | **authentication** | **privacy**] [**volatile** | **nonvolatile**]

Parameters

paramsname	Specifies a name identifying parameters used to generate SNMP messages to a particular target.
user *user*	Specifies an SNMPv1 or v2 community name or an SNMPv3 user name. Maximum length is 32 bytes.

Downloaded from www.Manualslib.com manuals search engine

security-model v1 | v2c | usm	Specifies the SNMP security model applied to this target parameter as version 1, 2c or 3 (usm).
message-processing v1 | v2c | v3	Specifies the SNMP message processing model applied to this target parameter as version 1, 2c or 3.
noauthentication | authentication | privacy	(Optional) Specifies the SNMP security level applied to this target parameter as no authentication, authentication (without privacy) or privacy. Privacy specifies that messages sent on behalf of the user are protected from disclosure.
volatile | nonvolatile	(Optional) Specifies the storage type applied to this target parameter.

Defaults

None.

- If not specified, security level will be set to **noauthentication.**
- If not specified, storage type will be set to **nonvolatile**.

Mode

Switch command, Read-Write.

Example

This example shows how to set SNMP target parameters named "v1ExampleParams" for a user named "fred" using version 3 security model and message processing, and authentication*:*

```
Matrix(rw)->set snmp targetparams v1ExampleParams user fred security-model usm
message-processing v3 authentication
```

clear snmp targetparams

Use this command to clear the SNMP target parameter configuration.

Syntax

clear snmp targetparams *targetParams*

Parameters

targetParams	Specifies the name of the parameter in the SNMP target parameters table to be cleared.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to clear SNMP target parameters named "v1ExampleParams":

```
Matrix(rw)->clear snmp targetparams v1ExampleParams
```


Downloaded from www.Manualslib.com manuals search engine

Configuring SNMP Target Addresses

Purpose

To review and configure SNMP target addresses which will receive SNMP notification messages. An address configuration can be linked to optional SNMP transmit, or target, parameters (such as timeout, retry count, and UDP port) set with the **set snmp targetparams** command ("set snmp targetparams" on page 5-27).

Commands

For information about...	Refer to page...
show snmp targetaddr	5-29
set snmp targetaddr	5-30
clear snmp targetaddr	5-31

show snmp targetaddr

Use this command to display SNMP target address information.

Syntax

show snmp targetaddr [*targetAddr*] [**volatile** | **nonvolatile** | **read-only**]

Parameters

targetAddr	(Optional) Displays information for a specific target address name.
volatile | **nonvolatile** | **read-only**	(Optional) When target address is specified, displays target address information for a specific storage type.

Defaults

- If *targetAddr* is not specified, entries for all target address names will be displayed.
- If not specified, entries of all storage types will be displayed for a target address.

Mode

Switch command, Read-Only.

Example

This example shows how to display SNMP target address information:

```
Matrix(rw)->show snmp targetaddr
Target Address Name     = labmachine
Tag List                = v2cTrap
IP Address              = 10.2.3.116
UDP Port#               = 162
Target Mask             = 255.255.255.255
Timeout                 = 1500
```


Downloaded from www.Manualslib.com manuals search engine

```
Retry count             = 4
Parameters              = v2cParams
Storage type            = nonVolatile
Row status              = active
```

Table 5-10 shows a detailed explanation of the command output.

Table 5-10 show snmp targetaddr Output Details

Output...	What it displays...
Target Address Name	Unique identifier in the snmpTargetAddressTable.
Tag List	Tags a location to the target address as a place to send notifications.
IP Address	Target IP address.
UDP Port#	Number of the UDP port of the target host to use.
Target Mask	Target IP address mask.
Timeout	Timeout setting for the target address.
Retry count	Retry setting for the target address.
Parameters	Entry in the snmpTargetParamsTable.
Storage type	Whether entry is stored in **volatile**, **nonvolatile**, or **read-only** memory.
Row status	Status of this entry: **active**, **notInService**, or **notReady**.

set snmp targetaddr

Use this command to configure an SNMP target address.

Syntax

set snmp targetaddr *targetaddr ipaddr* **param** *param* [**udpport** *udpport*] [**mask** *mask*] [**timeout** *timeout*] [**retries** *retries*] [**taglist** *taglist*] [**volatile** | **nonvolatile**]

Parameters

targetaddr	Specifies a unique identifier to index the snmpTargetAddrTable. Maximum length is 32 bytes.
ipaddr	Specifies the IP address of the target.
param *param*	Specifies an entry in the SNMP target parameters table, which is used when generating a message to the target. Maximum length is 32 bytes.
udpport *udpport*	(Optional) Specifies which UDP port of the target host to use.
mask *mask*	(Optional) Specifies the IP mask of the target.
timeout *timeout*	(Optional) Specifies the maximum round trip time allowed to communicate to this target address. This value is in .01 seconds and the default is 1500 (15 seconds.)
retries *retries*	(Optional) Specifies the number of message retries allowed if a response is not received. Default is 3.

Downloaded from www.Manualslib.com manuals search engine

taglist *taglist*	(Optional) Specifies a list of SNMP notify tag values. This tags a location to the target address as a place to send notifications. List must be enclosed in quotes and tag values must be separated by a space (i.e.: **"tag 1 tag 2"**)
volatile | **nonvolatile**	(Optional) Specifies temporary (default), or permanent storage for SNMP entries.

Defaults

- If not specified, *udpport* will be set to **162**.
- If not specified, *mask* will be set to **255.255.255.255**
- If not specified, *timeout* will be set to **1500**.
- If not specified, number of *retries* will be set to **3**.
- If **taglist** is not specified, none will be set.
- If not specified, storage type will be **nonvolatile**.

Mode

Switch command, Read-Write.

Usage

The target address is a unique identifier and a specific IP address that will receive SNMP notification messages and determine which community strings will be accepted. This address configuration can be linked to optional SNMP transmit parameters (such as timeout, retry count, and UDP port).

Example

This example shows how to configure a trap notification called "TrapSink." This trap notification will be sent to the workstation 192.168.190.80 (which is target address "tr"). It will use security and authorization criteria contained in a target parameters entry called "v2cExampleParams". For more information on creating a basic SNMP trap, refer to "Creating a Basic SNMP Trap Configuration" on page 5-3:

```
Matrix(rw)->set snmp targetaddr tr 192.168.190.80 param v2cExampleParams taglist
TrapSink
```

clear snmp targetaddr

Use this command to delete an SNMP target address entry.

Syntax

clear snmp targetaddr *targetAddr*

Parameters

targetAddr	Specifies the target address entry to delete.

Defaults

None.

Downloaded from www.Manualslib.com manuals search engine

Mode

Switch command, Read-Write.

Example

This example shows how to clear SNMP target address entry “tr”:

```
Matrix(rw)->clear snmp targetaddr tr
```


Downloaded from www.Manualslib.com manuals search engine

Configuring SNMP Notification Parameters

Purpose

To configure SNMP notification parameters and optional filters. Notifications are entities which handle the generation of SNMP v1 and v2 "traps" or SNMP v3 "informs" messages to select management targets. Optional notification filters identify which targets should not receive notifications. For a sample SNMP trap configuration showing how SNMP notification parameters are associated with security and authorization criteria (target parameters) and mapped to a management target address, refer to "Creating a Basic SNMP Trap Configuration" on page 5-3.

About SNMP Notify Filters

Profiles indicating which targets should not receive SNMP notification messages are kept in the NotifyFilter table. If this table is empty, meaning that no filtering is associated with any SNMP target, then no filtering will take place. "Traps" or "informs" notifications will be sent to all destinations in the SNMP targetAddrTable that have tags matching those found in the NotifyTable.

When the NotifyFilter table contains profile entries, the SNMP agent will find any filter profile name that corresponds to the target parameter name contained in an outgoing notification message. It will then apply the appropriate subtree-specific filter when generating notification messages.

Commands

For information about...	Refer to page...
show snmp notify	5-33
set snmp notify	5-35
clear snmp notify	5-35
show snmp notifyfilter	5-36
set snmp notifyfilter	5-37
clear snmp notifyfilter	5-37
show snmp notifyprofile	5-38
set snmp notifyprofile	5-39
clear snmp notifyprofile	5-39

show snmp notify

Use this command to display the SNMP notify configuration, which determines which management targets will receive SNMP notifications.

Syntax

show snmp notify [*notify*] [**volatile** | **nonvolatile** | **read-only**]

Downloaded from www.Manualslib.com manuals search engine

Parameters

notify	(Optional) Displays notify entries for a specific notify name.
volatile | **nonvolatile** | **read-only**	(Optional) Displays notify entries for a specific storage type.

Defaults

- If a *notify* name is not specified, all entries will be displayed.
- If **volatile**, **nonvolatile** or **read-only** are not specified, all storage type entries will be displayed.

Mode

Switch command, Read-Only.

Example

This example shows how to display the SNMP notify information:

```
Matrix(rw)->show snmp notify

 --- SNMP notifyTable information ---
Notify name     = 1
Notify Tag      = Console
Notify Type     = trap
Storage type    = nonVolatile
Row status      = active

Notify name     = 2
Notify Tag      = TrapSink
Notify Type     = trap
Storage type    = nonVolatile
Row status      = active
```

Table 5-11 shows a detailed explanation of the command output.

Table 5-11 show snmp notify Output Details

Output...	What it displays...
Notify name	A unique identifier used to index the SNMP notify table.
Notify Tag	Name of the entry in the SNMP notify table.
Notify Type	Type of notification: SNMPv1 or v2 **trap** or SNMPv3 **InformRequest** message.
Storage type	Whether access entry is stored in **volatile**, **nonvolatile** or **read-only** memory.
Row status	Status of this entry: **active**, **notInService,** or **notReady**.

Downloaded from www.Manualslib.com manuals search engine

set snmp notify

Use this command to set the SNMP notify configuration.

Syntax

set snmp notify *notify* **tag** *tag* [**trap** | **inform**] [**volatile** | **nonvolatile**]

Parameters

notify	Specifies an SNMP notify name.
tag *tag*	Specifies an SNMP notify tag. This binds the notify name to the SNMP target address table.
trap | **inform**	(Optional) Specifies SNMPv1 or v2 Trap messages (default) or SNMP v3 InformRequest messages.
volatile | **nonvolatile**	(Optional) Specifies temporary (default), or permanent storage for SNMP entries.

Defaults

- If not specified, message type will be set to **trap**.
- If not specified, storage type will be set to **nonvolatile**.

Mode

Switch command, Read-Write.

Usage

This creates an entry in the SNMP notify table, which is used to select management targets who should receive notification messages. This command's **tag** parameter can be used to bind each entry to a target address using the **set snmp targetaddr** command ("set snmp targetaddr" on page 5-30).

Example

This example shows how to set an SNMP notify configuration with a notify name of "hello" and a notify tag of "world". Notifications will be sent as trap messages and storage type will automatically default to permanent:

```
Matrix(rw)->set snmp notify hello tag world trap
```

clear snmp notify

Use this command to clear an SNMP notify configuration.

Syntax

clear snmp notify *notify*

Parameters

notify	Specifies an SNMP notify name to clear.

Downloaded from www.Manualslib.com manuals search engine

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to clear the SNMP notify configuration for “hello”:

```
Matrix(rw)->clear snmp notify hello
```

show snmp notifyfilter

Use this command to display SNMP notify filter information, identifying which profiles will not receive SNMP notifications.

Syntax

show snmp notifyfilter [*profile*] [**subtree** *oid-or-mibobject*] [**volatile** | **nonvolatile** | **read-only**]

Parameters

profile	(Optional) Displays a specific notify filter.
subtree *oid-or-mibobject*	(Optional) Displays a notify filter within a specific subtree.
volatile | **nonvolatile** | **read-only**	(Optional) Displays notify filter entries of a specific storage type.

Defaults

If no parameters are specified, all notify filter information will be displayed.

Mode

Switch command, Read-Only.

Example

This example shows how to display SNMP notify filter information. In this case, the notify profile “pilot1” in subtree 1.3.6 will not receive SNMP notification messages:

```
Matrix(rw)->show snmp notifyfilter

--- SNMP notifyFilter information ---
Profile         = pilot1
Subtree         = 1.3.6
Filter type     = included
Storage type    = nonVolatile
Row status      = active
```


Downloaded from www.Manualslib.com manuals search engine

set snmp notifyfilter

Use this command to create an SNMP notify filter configuration.

Syntax

set snmp notifyfilter *profile* **subtree** *oid-or-mibobject* [**mask** *mask*] [**included** | **excluded**] [**volatile** | **nonvolatile**]

Parameters

profile	Specifies an SNMP filter notify name.
subtree *oid-or-mibobject*	Specifies a MIB subtree ID target for the filter.
mask *mask*	(Optional) Applies a subtree mask.
included | **excluded**	(Optional) Specifies that subtree is included or excluded.
volatile | **nonvolatile**	(Optional) Specifies a storage type.

Defaults

- If not specified, **mask** is not set.
- If not specified, subtree will be **included**.
- If storage type is not specified, **nonvolatile** (permanent) will be applied.

Mode

Switch command, Read-Write.

Usage

This identifies which management targets should NOT receive notification messages, which is useful for fine-tuning the amount of SNMP traffic generated.

Example

This example shows how to create an SNMP notify filter called “pilot1” with a MIB subtree ID of 1.3.6:

```
Matrix(rw)->set snmp notifyfilter pilot1 subtree 1.3.6
```

clear snmp notifyfilter

Use this command to delete an SNMP notify filter configuration.

Syntax

clear snmp notifyfilter *profile* **subtree** *oid-or-mibobject*

Parameters

profile	Specifies an SNMP filter notify name to delete.
subtree *oid-or-mibobject*	Specifies a MIB subtree ID containing the filter to be deleted.

Downloaded from www.Manualslib.com manuals search engine

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to delete the SNMP notify filter “pilot1”:

```
Matrix(rw)->clear snmp notifyfilter pilot1 subtree 1.3.6
```

show snmp notifyprofile

Use this command to display SNMP notify profile information. This associates target parameters to an SNMP notify filter to determine who should not receive SNMP notifications.

Syntax

show snmp notifyprofile [*profile*] [**targetparam** *targetparam*] [**volatile** | **nonvolatile** | **read-only**]

Parameters

profile	(Optional) Displays a specific notify profile.
targetparam *targetparam*	(Optional) Displays entries for a specific target parameter.
volatile | **nonvolatile** | **read-only**	(Optional) Displays notify filter entries of a specific storage type.

Defaults

If no parameters are specified, all notify profile information will be displayed.

Mode

Switch command, Read-Only.

Example

This example shows how to display SNMP notify information for the profile named “area51”:

```
Matrix(rw)->show snmp notifyprofile area51

 --- SNMP notifyProfile information ---
Notify Profile  = area51
TargetParam     = v3ExampleParams
Storage type    = nonVolatile
Row status      = active
```


Downloaded from www.Manualslib.com manuals search engine

set snmp notifyprofile

Use this command to create an SNMP notify filter profile configuration.

Syntax

set snmp notifyprofile *profile* **targetparam** *targetparam* [**volatile** | **nonvolatile**]

Parameters

profile	Specifies an SNMP filter notify name.
targetparam *targetparam*	Specifies an associated entry in the SNMP Target Params Table.
volatile | **nonvolatile**	(Optional) Specifies a storage type.

Defaults

If storage type is not specified, **nonvolatile** (permanent) will be applied.

Mode

Switch command, Read-Write.

Usage

This associates a notification filter, created with the **set snmp notifyfilter** command ("set snmp notifyfilter" on page 5-37), to a set of SNMP target parameters to determine which management targets should not receive SNMP notifications.

Example

This example shows how to create an SNMP notify profile named area51 and associate a target parameters entry.

```
Matrix(rw)->set snmp notifyprofile area51 targetparam v3ExampleParams
```

clear snmp notifyprofile

Use this command to delete an SNMP notify profile configuration.

Syntax

clear snmp notifyprofile *profile* **targetparam** *targetparam*

Parameters

profile	Specifies an SNMP filter notify name to delete.
targetparam *targetparam*	Specifies an associated entry in the snmpTargetParamsTable.

Defaults

None.

Mode

Switch command, Read-Write.

Downloaded from www.Manualslib.com manuals search engine

Example

This example shows how to delete SNMP notify profile “area51”:

```
Matrix(rw)->clear snmp notifyprofile area51 targetparam v3ExampleParams
```


Downloaded from www.Manualslib.com manuals search engine

Configuring SNMP Walk Behavior

Purpose

To configure SNMP walk behavior.

Commands

For information about...	Refer to page...
set snmp timefilter break	5-41

set snmp timefilter break

Use this command to set SNMP to exit the MIB walk after the first entry it returns if the index includes a timestamp.

Syntax

set snmp timefilter break {**enable** | **disable**}

Parameters

enable	Configures the MIB walk behavior to exit after the first entry is returned when the getNext object index contains a timestamp.
disable	Configures the MIB walk behavior to only exit when the current time is reached when the getNext object index contains a timestamp.

Defaults

Disabled.

Mode

Switch command, Read-Write.

Usage

When an index contains a timestamp, by default the getNext walk continues to return values until the current time is reached, which may not ever occur, leaving the user with the impression that the walk is in a loop. Enabling this command will exit the walk after the first entry is returned.

Examples

This example enables the SNMP timestamp filter break for this router:

```
Matrix(rw)->set snmp timefilter break enable
```


Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

6

Spanning Tree Configuration

This chapter describes the Spanning Tree Configuration set of commands and how to use them.

For information about...	Refer to page...
Overview: Single, Rapid and Multiple Spanning Tree Protocols	6-1
Configuring Spanning Tree Bridge Parameters	6-3
Configuring Spanning Tree Port Parameters	6-49
Configuring Spanning Tree Loop Protect Features	6-65

Overview: Single, Rapid and Multiple Spanning Tree Protocols

The IEEE 802.1D Spanning Tree Protocol (STP) resolves the problems of physical loops in a network by establishing one primary path between any two devices in a network. Any duplicate paths are barred from use and become standby or blocked paths until the original path fails, at which point they can be brought into service.

RSTP

The IEEE 802.1w Rapid Spanning Protocol (RSTP), an evolution of 802.1D, can achieve much faster convergence than legacy STP in a properly configured network. RSTP significantly reduces the time to reconfigure the network's active topology when physical topology or configuration parameter changes occur. It selects one switch as the root of a Spanning Tree-connected active topology and assigns port roles to individual ports on the switch, depending on whether that port is part of the active topology.

RSTP provides rapid connectivity following the failure of a switch, switch port, or a LAN. A new root port and the designated port on the other side of the bridge transition to forwarding through an explicit handshake between them. By default, user ports are configured to rapidly transition to forwarding in RSTP.

MSTP

The IEEE 802.1s Multiple Spanning Tree Protocol (MSTP) builds upon 802.1D and RSTP by optimizing utilization of redundant links between switches in a network. When redundant links exist between a pair of switches running single STP, one link is forwarding while the others are blocking for all traffic flowing between the two switches. The blocking links are effectively used only if the forwarding link goes down. MSTP assigns each VLAN present on the network to a particular Spanning Tree instance, allowing each switch port to be in a distinct state for each such instance: blocking for one Spanning Tree while forwarding for another. Thus, traffic associated with one set of VLANs can traverse a particular inter-switch link, while traffic associated with another set of VLANs can be blocked on that link. If VLANs are assigned to Spanning Trees wisely, no inter-switch link will be completely idle, maximizing network utilization.

Downloaded from www.Manualslib.com manuals search engine

For details on creating Spanning Tree instances, refer to “set spantree msti” on page 6-14.

For details on mapping Spanning Tree instances to VLANs, refer to “set spantree mstmap” on page 6-15.



Note: MSTP and RSTP are fully compatible and interoperable with each other and with legacy STP 802.1D.

Spanning Tree Features

The Matrix Series device meets the requirements of the Spanning Tree Protocols by performing the following functions:

- Creating a single Spanning Tree from any arrangement of switching or bridging elements.
- Compensating automatically for the failure, removal, or addition of any device in an active data path.
- Achieving port changes in short time intervals, which establishes a stable active topology quickly with minimal network disturbance.
- Using a minimum amount of communications bandwidth to accomplish the operation of the Spanning Tree Protocol.
- Reconfiguring the active topology in a manner that is transparent to stations transmitting and receiving data packets.
- Managing the topology in a consistent and reproducible manner through the use of Spanning Tree Protocol parameters.

Loop Protect

The Loop Protect feature prevents or short circuits loop formation in a network with redundant paths by requiring ports to receive type 2 BPDUs (RSTP/MSTP) on point-to-point inter-switch links (ISLs) before their states are allowed to become forwarding. Further, if a BPDU timeout occurs on a port, its state becomes listening until a BPDU is received.

Both upstream and downstream facing ports are protected. When a root or alternate port loses its path to the root bridge due to a message age expiration it takes on the role of designated port. It will not forward traffic until a BPDU is received. When a port is intended to be the designated port in an ISL it constantly proposes and will not forward until a BPDU is received, and will revert to listening if it fails to get a response. This protects against misconfiguration and protocol failure by the connected bridge.

The Disputed BPDU mechanism protects against looping in situations where there is one way communication. A disputed BPDU is one in which the flags field indicates a designated role and learning and the priority vector is worse than that already held by the port. If a disputed BPDU is received, the port is forced to the listening state. When an inferior designated BPDU with the learning bit set is received on a designated port, its state is set to discarding to prevent loop formation. Note that the Dispute mechanism is always active regardless of the configuration setting of Loop Protection.

Loop Protect operates as a per port, per MST instance feature. It should be set on inter-switch links. It is comprised of several related functions:

- Control of port forwarding state based on reception of agreement BPDUs
- Control of port forwarding state based on reception of disputed BPDUs
- Communicating port non-forwarding status through traps and syslog messages

Downloaded from www.Manualslib.com manuals search engine

- Disabling a port based on frequency of failure events

Port forwarding state in the designated port is gated by a timer that is set upon BPDU reception. It is analogous to the rcvdInfoWhile timer the port uses when receiving root information in the root/alternate/backup role.

There are two operational modes for Loop Protect on a port. If the port is connected to a device known to implement Loop Protect, it uses full functional mode. Otherwise the port operates in limited functional mode.

Connection to a Loop Protect switch guarantees that the alternate agreement mechanism is implemented. This means the designated port can rely on receiving a response to its proposal regardless of the role of the connected port, which has two important implications. First, the designated port connected to a non-root port may transition to forwarding. Second, there is no ambiguity when a timeout happens; a Loop Protect event has occurred.

In full functional mode, when a type 2 BPDU is received and the port is designated and point-to-point, the timer is set to 3 times helloTime. In limited functional mode there is the additional requirement that the flags field indicate a root role. If the port is a boundary port the MSTIs for that port follow the CIST, that is, the MSTI port timers are set according to the CIST port timer. If the port is internal to the region then the MSTI port timers are set independently using the particular MSTI message.

Message age expiration and the expiration of the Loop Protect timer are both Loop Protect events. A notice level syslog message is produced for each such event. Traps may be configured to report these events as well. A syslog message and trap may be configured for disputed BPDUs.

It is also configurable to force the locking of a SID/port for the occurrence of one or more events. When the configured number of events happen within a given window of time, the port is forced into blocking and held there until it is manually unlocked via management.

Note: Spanning Tree configuration should be performed only by personnel who are very knowledgeable about Spanning Trees and the configuration of the Spanning Tree Algorithm. Otherwise, the proper operation of the network could be at risk.

Configuring Spanning Tree Bridge Parameters

Purpose

To display and set Spanning Tree bridge parameters, including device priorities, hello time, maximum wait time, forward delay, path cost, and topology change trap suppression.

Note: The term “bridge” is used as an equivalent to the term “switch” or “device” in this document.

Commands

For information about...	Refer to page...
show spantree stats	6-6
show spantree version	6-9
set spantree version	6-9

Downloaded from www.Manualslib.com manuals search engine

For information about...	Refer to page...
clear spantree version	6-10
show spantree stpmode	6-10
set spantree stpmode	6-11
clear spantree stpmode	6-11
show spantree maxconfigurablestps	6-12
set spantree maxconfigurablestps	6-12
clear spantree maxconfigurablestps	6-13
show spantree mstilist	6-13
set spantree msti	6-14
clear spantree msti	6-14
show spantree mstmap	6-15
set spantree mstmap	6-15
clear spantree mstmap	6-16
show spantree vlanlist	6-16
show spantree mstcfgid	6-17
set spantree mstcfgid	6-17
clear spantree mstcfgid	6-18
show spantree bridgeprioritymode	6-18
set spantree bridgeprioritymode	6-19
clear spantree bridgeprioritymode	6-19
show spantree priority	6-20
set spantree priority	6-20
clear spantree priority	6-22
show spantree bridgehellomode	6-22
set spantree bridgehellomode	6-23
clear spantree bridgehellomode	6-23
show spantree hello	6-24
set spantree hello	6-24
clear spantree hello	6-25
show spantree maxage	6-25
set spantree maxage	6-26
clear spantree maxage	6-26
show spantree fwddelay	6-27
set spantree fwddelay	6-27
clear spantree fwddelay	6-28
show spantree autoedge	6-28

Downloaded from www.Manualslib.com manuals search engine

For information about...	Refer to page...
set spantree autoedge	6-29
clear spantree autoedge	6-29
show spantree legacypathcost	6-30
set spantree legacypathcost	6-30
clear spantree legacypathcost	6-31
show spantree tctrapsuppress	6-31
set spantree tctrapsuppress	6-32
clear spantree tctrapsuppress	6-32
show spantree txholdcount	6-33
set spantree txholdcount	6-33
clear spantree txholdcount	6-34
show spantree maxhops	6-34
set spantree maxhops	6-35
clear spantree maxhops	6-35
show spantree spanguard	6-36
set spantree spanguard	6-36
clear spantree spanguard	6-37
show spantree spanguardtimeout	6-37
set spantree spanguardtimeout	6-38
clear spantree spanguardtimeout	6-38
show spantree spanguardlock	6-39
clear / set spantree spanguardlock	6-39
show spantree spanguardtrapenable	6-40
set spantree spanguardtrapenable	6-40
clear spantree spanguardtrap enable	6-41
show spantree backuproot	6-41
set spantree backuproot	6-42
clear spantree backuproot	6-42
show spantree backuproottrapendable	6-43
set spantree backuproottrapenable	6-43
clear spantree backuproottrapenable	6-44
show spantree newroottrapendable	6-44
set spantree newroottrapenable	6-45
clear spantree newroottrapenable	6-45
clear spantree default	6-46

Downloaded from www.Manualslib.com manuals search engine

For information about...	Refer to page...
show spantree debug	6-46
clear spantree debug	6-48

show spantree stats

Use this command to display Spanning Tree information for one or more ports.

Syntax

show spantree stats [**port** *port-string*] [**sid** *sid*] [**active**]

Parameters

port *port-string*	(Optional) Displays information for the specified port(s). For a detailed description of possible *port--string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.
sid sid	(Optional) Displays information for a specific Spanning Tree identifier. If not specified, SID 0 is assumed.
active	(Optional) Displays information for ports that have received STP BPDUs since boot.

Defaults

- If *port-string* is not specified, Spanning Tree information for all ports will be displayed.
- If *sid* is not specified, information for Spanning Tree 0 will be displayed.
- If **active** is not specified information for all ports will be displayed regardless of whether or not they have received BPDUs.

Mode

Switch command, Read-Only.

Example

This example shows how to display the device's Spanning Tree configuration:

```
Matrix(rw)->show spantree stats

Spanning tree status          - enabled
Spanning tree instance        - 0
Designated Root MacAddr       - 00-e0-63-9d-c1-c8
Designated Root Priority      - 0
Designated Root Cost          - 10000
Designated Root Port          - lag.0.1
Root Max Age                  - 20 sec
Root Hello Time               - 2  sec
Root Forward Delay            - 15 sec
Bridge ID MAC Address         - 00-01-f4-da-5e-3d
Bridge ID Priority            - 32768
```


Downloaded from www.Manualslib.com manuals search engine

```
Bridge Max Age              - 20 sec
Bridge Hello Time           - 2  sec
Bridge Forward Delay        - 15 sec
Topology Change Count       - 7
Time Since Top Change       - 00 days 03:19:15
Max Hops                    - 20
```

Table 6-1 shows a detailed explanation of command output.

Table 6-1 show spantree Output Details

Output...	What it displays...
Spanning tree instance	Spanning Tree ID.
Spanning tree status	Whether Spanning Tree is enabled or disabled.
Designated Root MacAddr	MAC address of the designated Spanning Tree root bridge.
Designated Root Port	Port through which the root bridge can be reached.
Designated Root Priority	Priority of the designated root bridge.
Designated Root Cost	Total path cost to reach the root.
Root Max Age	Amount of time (in seconds) a BPDU packet should be considered valid.
Root Hello Time	Interval (in seconds) at which the root device sends BPDU (Bridge Protocol Data Unit) packets.
Root Forward Delay	Amount of time (in seconds) the root device spends in listening or learning mode.
Bridge ID MAC Address	Unique bridge MAC address, recognized by all bridges in the network.
Bridge ID Priority	Bridge priority, which is a default value, or is assigned using the **set spantree priority** command. For details, refer to “set spantree priority” on page 6-20.
Bridge Max Age	Maximum time (in seconds) the bridge can wait without receiving a configuration message (bridge “hello”) before attempting to reconfigure. This is a default value, or is assigned using the **set spantree maxage** command. For details, refer to “set spantree maxage” on page 6-26.
Bridge Hello Time	Amount of time (in seconds) the bridge sends BPDUs. This is a default value, or is assigned using the **set spantree hello** command. For details, refer to “set spantree hello” on page 6-24.
Bridge Forward Delay	Amount of time (in seconds) the bridge spends in listening or learning mode. This is a default value, or is assigned using the **set spantree fwddelay** command. For details, refer to “set spantree fwddelay” on page 6-27.
Topology Change Count	Number of times topology has changed on the bridge.
Time Since Top Change	Amount of time (in days, hours, minutes and seconds) since the last topology change.
Max Hops	Maximum number of hops information for a particular Spanning Tree instance may traverse (via relay of BPDUs within the applicable MST region) before being discarded. This is a default value, or is assigned using the **set spantree mashops** command. For details, refer to “set spantree maxhops” on page 6-35.

Downloaded from www.Manualslib.com manuals search engine

This example shows how to display port-specific Spanning Tree information for port ge.1.1. Table 6-2 describes the port-specific information displayed.

```
Matrix(rw)->show spantree stats port ge.1.1

Spanning tree status          - enabled
Spanning tree instance        - 0
Designated Root MacAddr       - 00-e0-63-93-79-0f
Designated Root Priority      - 0
Designated Root Cost          - 0
Designated Root Port          - 0
Root Max Age                  - 20 sec
Root Hello Time               - 2  sec
Root Forward Delay            - 15 sec
Bridge ID MAC Address         - 00-e0-63-93-79-0f
Bridge ID Priority            - 0
Bridge Max Age                - 20 sec
Bridge Hello Time             - 2  sec
Bridge Forward Delay          - 15 sec
Topology Change Count         - 5
Time Since Top Change         - 00 days 03:16:54
Max Hops                      - 20

SID   Port         State              Role          Cost        Priority
---   ----------   ----------------   -----------   --------    --------
0     ge.1.1       Blocking           Disabled      20000       128
```

Table 6-2 Port-Specific show spantree stats Output Details

Output...	What it displays...
SID	The Spanning Tree instance.
Port	The port name.
State	The Spanning Tree forwarding state of the port. This value can be Blocking, Forwarding, Listening, or Learning. If the port/SID has been placed in a non-forwarding state for a reason other than normal Spanning Tree protocol operation, an asterisk will be displayed next to the state. You can use the show spantree nonforwardingreason command (“show spantree nonforwardingreason” on page 6-77) to display the specific reason.
Role	The Spanning Tree role of the port. The port role is assigned by the Spanning Tree protocol and determines the behavior of the port — either sending or receiving BPDUs, and forwarding or blocking data traffic.
Cost	The port cost.
Priority	The priority of the link in a Spanning Tree bridge. This value can be set with the set spantree portpri command (“set spantree portpri” on page 6-55).

Downloaded from www.Manualslib.com manuals search engine

show spantree version

Use this command to display the current version of the Spanning Tree protocol running on the device.

Syntax

```
show spantree version
```

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Only.

Example

This example shows how to display Spanning Tree version information for the device:

```
Matrix(rw)->show spantree version
Force Version is mstp
```

set spantree version

Use this command to set the version of the Spanning Tree protocol to MSTP (Multiple Spanning Tree Protocol), RSTP (Rapid Spanning Tree Protocol) or to STP 802.1D-compatible.

Syntax

```
set spantree version {mstp | stpcompatible | rstp}
```

Parameters

mstp	Sets the version to STP 802.1s-compatible.
stpcompatible	Sets the version to STP 802.1D-compatible.
rstp	Sets the version to 802.1w-compatible.

Defaults

None.

Mode

Switch command, Read-Write.

Usage

In most networks, Spanning Tree version should not be changed from its default setting of **mstp** (Multiple Spanning Tree Protocol) mode. MSTP mode is fully compatible and interoperable with legacy STP 802.1D and Rapid Spanning Tree (RSTP) bridges. Setting the version to **stpcompatible**

Downloaded from www.Manualslib.com manuals search engine

mode will cause the bridge to transmit only 802.1D BPDUs, and will prevent non-edge ports from rapidly transitioning to forwarding state.

Example

This example shows how to globally change the Spanning Tree version from the default of MSTP to RSTP:

```
Matrix(rw)->set spantree version rstp
```

clear spantree version

Use this command to reset the Spanning Tree version to MSTP mode.

Syntax

clear spantree version

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to reset the Spanning Tree version:

```
Matrix(rw)->clear spantree version
```

show spantree stpmode

Use this command to display the Spanning Tree Protocol (STP) mode setting.

Syntax

show spantree stpmode

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Only.

Downloaded from www.Manualslib.com manuals search engine

Example

This example shows how to display the STP mode:

```
Matrix(rw)->show spantree stpmode
Bridge Stp Mode is set to ieee8021
```

set spantree stpmode

Use this command to globally enable or disable the Spanning Tree Protocol (STP) mode.

Syntax

set spantree stpmode {**none** | **ieee8021**}

Parameters

none	Disables Spanning Tree.
ieee8021	Enables 802.1 Spanning Tree mode.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to disable Spanning Tree:

```
Matrix(rw)->set spantree stpmode none
```

clear spantree stpmode

Use this command to reset the Spanning Tree protocol mode to the default setting of IEEE802.1. This re-enables Spanning Tree.

Syntax

clear spantree stpmode

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Write.

Downloaded from www.Manualslib.com manuals search engine

Example

This example shows how to reset the STP mode to IEEE 802.1:

```
Matrix(rw)->clear spantree stpmode
```

show spantree maxconfigurablestps

Use this command to display the setting for the maximum number of user configurable Spanning Tree instances.

Syntax

show spantree maxconfigurablestps

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Only.

Example

This example shows how to display the STP maximum configs setting:

```
Matrix(rw)->show spantree maxconfigurablestps
Max user configurable stps is set to 33
```

set spantree maxconfigurablestps

Use this command to set the maximum number of user configurable Spanning Tree instances.

Syntax

set spantree maxconfigurablestps *numstps*

Parameters

numstps	Specifies the maximum number of user configured STPs to be allowed on this bridge. Valid values are 1 - 9.

Defaults

None.

Mode

Switch command, Read-Write.

Downloaded from www.Manualslib.com manuals search engine

Example

This example shows how to set the STP max configs to 8:

```
Matrix(rw)->set spantree maxconfigurablestps 8
```

clear spantree maxconfigurablestps

Use this command to clear the setting for the maximum number of user configurable Spanning Tree instances.

Syntax

clear spantree maxconfigurablestps

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to clear the STP max configs setting:

```
Matrix(rw)->clearspantree maxconfigurablestps
```

show spantree mstilist

Use this command to display a list of Multiple Spanning Tree (MST) instances configured on the device.

Syntax

show spantree mstilist

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Only.

Example

This example shows how to display a list of MST instances. In this case, SID 2 has been configured:

```
Matrix(rw)->show spantree mstilist
 Configured Multiple Spanning Tree instances: 2
```


Downloaded from www.Manualslib.com manuals search engine

set spantree msti

Use this command to create or delete a Multiple Spanning Tree instance.

Syntax

set spantree msti sid *sid* {**create** | **delete**}

Parameters

sid *sid*	Sets the Multiple Spanning Tree ID. Valid values are **1** - **4094**. **Note:** Matrix Series devices will support up to 32 instances with an additional 128 MB of memory installed.
create | **delete**	Creates or deletes an MST instance.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to create MST instance 2:

```
Matrix(rw)->set spantree msti sid 2 create
```

clear spantree msti

Use this command to delete one or more Multiple Spanning Tree instances.

Syntax

clear spantree msti *sid*

Parameters

sid	Specifies a multiple Spanning Tree ID to be deleted.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to delete MST instance 1:

```
Matrix(rw)->clear spantree msti 1
```


Downloaded from www.Manualslib.com manuals search engine

show spantree mstmap

Use this command to display the mapping of a filtering database ID (FID) to a Spanning Trees. Since VLANs are mapped to FIDs, this shows to which SID a VLAN is mapped.

Syntax

show spantree mstmap [**fid** *fid*]

Parameters

fid *fid*	(Optional) Displays information for specific FIDs.

Defaults

If *fid* is not specified, information for all assigned FIDs will be displayed.

Mode

Switch command, Read-Only.

Example

This example shows how to display SID to FID mapping information for FID 1. In this case, no new mappings have been configured:

```
Matrix(rw)->show spantree mstmap fid 1
FID:       SID:
1          0
```

set spantree mstmap

Use this command to map one or more filtering database IDs (FIDs) to a SID. Since VLANs are mapped to FIDs, this essentially maps one or more VLAN IDs to a Spanning Tree (SID).

Syntax

set spantree mstmap *fid* [**sid** *sid*]

Parameters

fid	Specifies one or more FIDs to assign to the MST. Valid values are **1** - **4093**, and must correspond to a VLAN ID created using the **set vlan** command as described in "set vlan" on page 7-6.
sid *sid*	(Optional) Specifies a Multiple Spanning Tree ID. Valid values are **1** - **4094**, and must correspond to a SID created using the **set msti** command as described in "set spantree msti" on page 6-14.

Defaults

If *sid* is not specified, FID(s) will be mapped to Spanning Tree 0.

Mode

Switch command, Read-Write.

Downloaded from www.Manualslib.com manuals search engine

Example

This example shows how to map FID 3 to SID 2:

```
Matrix(rw)->set spantree mstmap 3 sid 2
```

clear spantree mstmap

Use this command to map a FID back to SID 0.

Syntax

clear spantree mstmap *fid*

Parameters

fid	Specifies one or more FIDs to reset to 0.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to map FID 2 back to SID 0:

```
Matrix(rw)->clear spantree mstmap 2
```

show spantree vlanlist

Use this command to display the VLAN ID(s) assigned to one or more Spanning Trees.

Syntax

show spantree vlanlist [*vlan-list*]

Parameters

vlan-list	(Optional) Displays information for specific VLAN(s).

Defaults

If not specified, SID assignment will be displayed only for VLANs assigned to any SID other than SID 0.

Mode

Switch command, Read-Only.

Downloaded from www.Manualslib.com manuals search engine

Example

This example shows how to display assignments for all VLANs assigned to any SID other than SID 0:

```
Matrix(rw)->show spantree vlanlist
Vlan 104 is mapped to Sid 104
Vlan 105 is mapped to Sid 105
Vlan 106 is mapped to Sid 106
Vlan 107 is mapped to Sid 107
```

show spantree mstcfgid

Use this command to display the MST configuration identifier elements, including format selector, configuration name, revision level, and configuration digest.

Syntax

show spantree mstcfgid

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Only.

Example

This example shows how to display the MST configuration identifier elements. In this case, the default revision level of 0, and the default configuration name (a string representing the bridge MAC address) have not been changed. For information on using the **set spantree mstcfgid** command to change these settings, refer to "set spantree mstcfgid" on page 6-17:

```
Matrix(rw)->show spantree mstcfgid
 MST Configuration Identifier:
  Format Selector: 0
  Configuration Name: 00:01:f4:89:51:94
  Revision Level: 0
  Configuration Digest: ac:36:17:7f:50:28:3c:d4:b8:38:21:d8:ab:26:de:62
```

set spantree mstcfgid

Use this command to set the MST configuration name and/or revision level.

Syntax

set spantree mstcfgid {**cfgname** *name* | **rev** *level*}

Downloaded from www.Manualslib.com manuals search engine

Parameters

cfgname *name*	Specifies an MST configuration name.
rev *level*	Specifies an MST revision level. Valid values are **0** - **65535**.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to set the MST configuration name to “mstconfig”:

```
Matrix(rw)->set spantree mstconfigid cfgname mstconfig
```

clear spantree mstcfgid

Use this command to reset the MST revision level to a default value of 0, and the configuration name to a default string representing the bridge MAC address.

Syntax

clear spantree mstcfgid

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to reset the MST configuration identifier elements to default values:

```
Matrix(rw)->clear spantree mstcfgid
```

show spantree bridgeprioritymode

Use this command to display the Spanning Tree bridge priority mode setting.

Syntax

show spantree bridgeprioritymode

Parameters

None.

Downloaded from www.Manualslib.com manuals search engine

Defaults

None.

Mode

Switch command, Read-Only.

Example

This example shows how to display the Spanning Tree bridge priority mode setting:

```
Matrix(rw)->show spantree bridgeprioritymode
Bridge Priority Mode is set to IEEE802.1t mode.
```

set spantree bridgeprioritymode

Use this command to set the Spanning Tree bridge priority mode to 802.1D (legacy) or 802.1t. This will affect the range of priority values used to determine which device is selected as the Spanning Tree root as described in **set spantree priority** ("set spantree priority" on page 6-20).

Syntax

```
set spantree bridgeprioritymode {8021d | 8021t}
```

Parameters

8021d	Sets the bridge priority mode to use 802.1D (legacy) values of values, which are 0 - 65535.
8021t	Sets the bridge priority mode to use 802.1t values, which are 0 - 61440, in increments of 4096. Values will be rounded up or down, depending on the 802.1t value to which the entered value is closest.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to set the bridge priority mode to 802.1D:

```
Matrix(rw)->set spantree bridgeprioritymode 8021d
```

clear spantree bridgeprioritymode

Use this command to reset the Spanning Tree bridge priority mode to the default setting of 802.1t.

Syntax

```
clear spantree bridgeprioritymode
```

Parameters

None.

Downloaded from www.Manualslib.com manuals search engine

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to reset the bridge priority mode to 802.1t:

```
Matrix(rw)->clear spantree bridgeprioritymode
```

show spantree priority

Use this command to display the Spanning Tree bridge priority.

Syntax

show spantree priority [*sid*]

Parameters

sid	(Optional) Displays the priority for a specific Spanning Tree. Valid values are **0** - **4094**. If not specified, SID 0 is assumed.

Defaults

If *sid* is not specified, priority will be shown for Spanning Tree 0.

Mode

Switch command, Read-Only.

Example

This example shows how to show the bridge priority for Spanning Tree 0

```
Matrix(rw)->show spantree priority
Bridge Priority is set to 4096 on sid 0
```

set spantree priority

Use this command to set the device's Spanning Tree priority.

Syntax

set spantree priority *priority* [*sid*]

Downloaded from www.Manualslib.com manuals search engine

Parameters

priority	Specifies the priority of the bridge. Valid values are from **0** to **65535,** with the numerical value of 0 indicating highest priority and the numerical value 65535 indicating lowest priority. When 802.1t is selected as the bridge priority mode, as described in "set spantree bridgeprioritymode" on page 6-19, values will be rounded up or down, depending on the 802.1t value to which the entered value is closest, in increments of 4096.
sid	(Optional) Sets the priority on a specific Spanning Tree. Valid values are **0** - **4094**. If not specified, SID 0 is assumed.

Defaults

If *sid* is not specified, priority will be set on Spanning Tree 0.

Mode

Switch command, Read-Write.

Usage

The device with the highest priority (lowest numerical value) becomes the Spanning Tree root device. If all devices have the same priority, the device with the lowest MAC address will then become the root device. Depending on the **set bridgepriority mode** setting as described in "set spantree bridgeprioritymode" on page 6-19, some priority values may be translated, and the translation will display in the CLI output as shown in the examples in this section.

Examples

This example shows how to set the bridge priority to 1 on all SIDs with 8021t priority mode enabled:

```
Matrix(rw)->set spantree priority 1
Bride Priority has been translated to incremental step of 4096
```

This example shows how to set the bridge priority to 15 on all SIDs with 8021t priority mode enabled:

```
Matrix(rw)->set spantree priority 15
Bride Priority has been translated to incremental step of 61440
```

This example shows how to set the bridge priority to 4000 on all SIDs with 8021t priority mode enabled:

```
Matrix(rw)->set spantree priority 4000
Bride Priority has been rounded up to 4096 from 4000
```

This example shows how to set the bridge priority to 10000 on all SIDs with 8021t priority mode enabled:

```
Matrix(rw)->set spantree priority 10000
Bride Priority has been rounded down to 8192 from 10000
```

This example shows how to set the bridge priority to 1000 on all SIDs with 8021t priority mode enabled:

```
Matrix(rw)->set spantree priority 1000
Bride Priority has been rounded down to 0 from 1000
```


Downloaded from www.Manualslib.com manuals search engine

clear spantree priority

Use this command to reset the Spanning Tree priority to the default value of 32768.

Syntax

clear spantree priority [*sid*]

Parameters

sid	(Optional) Resets the priority on a specific Spanning Tree. Valid values are **0** - **4094**. If not specified, SID 0 is assumed.

Defaults

If *sid* is not specified, priority will be reset on Spanning Tree 0.

Mode

Switch command, Read-Write.

Example

This example shows how to reset the bridge priority on SID 1:

```
Matrix(rw)->clear spantree priority 1
```

show spantree bridgehellomode

Use this command to display the status of bridge hello mode on the device.

Syntax

show spantree bridgehellomode

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Only.

Usage

When enabled, a single bridge administrative hello time is being used. When disabled, per-port administrative hello times are being used.

Downloaded from www.Manualslib.com manuals search engine

Example

This example shows how to display the Spanning Tree bridge hello mode. In this case, a single bridge hello mode has been enabled using the **set spantree bridgehellomode** command as described in "set spantree hello" on page 6-24:

```
Matrix(rw)->show spantree bridgehellomode
 Bridge Hello Mode is currently enabled.
```

set spantree bridgehellomode

Use this command to enable or disable bridge hello mode on the device.

Syntax

set spantree bridgehellomode {**enable** | **disable**}

Parameters

enable	Enables single Spanning Tree bridge hello mode.
disable	Disables single Spanning Tree bridge hello mode, allowing for the configuration of per-port hello times.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to disable single Spanning Tree hello mode on the device. Per-port hello times can now be configured using the **set spantree porthellomode** command as described in "set spantree porthello" on page 6-56:

```
Matrix(rw)->set spantree bridgehellomode disable
```

clear spantree bridgehellomode

Use this command to reset the Spanning Tree administrative hello mode to enabled.

Syntax

clear spantree bridgehellomode

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Write.

Downloaded from www.Manualslib.com manuals search engine

Example

This example shows how to reset the Spanning Tree bridge hello mode to enabled:

```
Matrix(rw)->clear spantree bridgehellomode
```

show spantree hello

Use this command to display the Spanning Tree hello time.

Syntax

show spantree hello

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Only.

Example

This example shows how to display the Spanning Tree hello time:

```
Matrix(rw)->show spantree hello
 Bridge Hello Time is set to 2 seconds
```

set spantree hello

Use this command to set the device's Spanning Tree hello time.

Syntax

set spantree hello *interval*

Parameters

interval	Specifies the number of seconds the system waits before broadcasting a bridge hello message (a multicast message indicating that the system is active). Valid values are **1** - **10**.

Defaults

None.

Mode

Switch command, Read-Write.

Usage

This is the time interval (in seconds) the device will transmit BPDUs indicating it is active.

Downloaded from www.Manualslib.com manuals search engine

Example

This example shows how to globally set the Spanning Tree hello time to 10 seconds:

```
Matrix(rw)->set spantree hello 10
```

clear spantree hello

Use this command to reset the Spanning Tree hello time to the default value.

Syntax

clear spantree hello

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to globally reset the Spanning Tree hello time:

```
Matrix(rw)->clear spantree hello
```

show spantree maxage

Use this command to display the Spanning Tree maximum aging time.

Syntax

show spantree maxage

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Only.

Example

This example shows how to display the Spanning Tree maximum aging time:

```
Matrix(rw)->show spantree maxage
 Bridge Max Age Time is set to 20 seconds
```


Downloaded from www.Manualslib.com manuals search engine

set spantree maxage

Use this command to set the bridge maximum aging time.

Syntax

set spantree maxage *agingtime*

Parameters

agingtime	Specifies the maximum number of seconds that the system retains the information received from other bridges through STP. Valid values are **6** - **40**.

Defaults

None

Mode

Switch command, Read-Write.

Usage

Maximum aging time is the maximum time (in seconds) a device can wait without receiving a configuration message (bridge "hello") before attempting to reconfigure. All device ports (except for designated ports) should receive configuration messages at regular intervals. Any port that ages out STP information provided in the last configuration message becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the device ports attached to the network.

Example

This example shows how to set the maximum aging time to 25 seconds:

```
Matrix(rw)->set spantree maxage 25
```

clear spantree maxage

Use this command to reset the maximum aging time for a Spanning Tree to the default value.

Syntax

clear spantree maxage

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Write.

Downloaded from www.Manualslib.com manuals search engine

Example

This example shows how to globally reset the maximum aging time:

```
Matrix(rw)->clear spantree maxage
```

show spantree fwddelay

Use this command to display the Spanning Tree forward delay time.

Syntax

show spantree fwddelay

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Only.

Example

This example shows how to display the Spanning Tree forward delay time:

```
Matrix(rw)->show spantree fwddelay
 Bridge Forward Delay is set to 15 seconds
```

set spantree fwddelay

Use this command to set the Spanning Tree forward delay.

Syntax

set spantree fwddelay *delay*

Parameters

delay	Specifies the number of seconds for the bridge forward delay. Valid values are **4** - **30**.

Defaults

None.

Mode

Switch command, Read-Write.

Usage

Spanning Tree forward delay is the maximum time (in seconds) the root device will wait before changing states (that is, listening to learning to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward frames. In

Downloaded from www.Manualslib.com manuals search engine

addition, each port needs time to listen for conflicting information that would make it return to a blocking state; otherwise, temporary data loops might result.

Example

This example shows how to globally set the bridge forward delay to 16 seconds:

```
Matrix(rw)->set spantree fwddelay 16
```

clear spantree fwddelay

Use this command to reset the Spanning Tree forward delay to the default setting of 15 seconds.

Syntax

clear spantree fwddelay

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to globally reset the bridge forward delay:

```
Matrix(rw)->clear spantree fwddelay
```

show spantree autoedge

Use this command to display the status of automatic edge port detection.

Syntax

show spantree autoedge

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Only.

Downloaded from www.Manualslib.com manuals search engine

Example

This example shows how to display the status of the automatic edge port detection function:

```
Matrix(rw)->show spantree autoedge
 autoEdge is currently enabled.
```

set spantree autoedge

Use this command to enable or disable the automatic edge port detection function.

Syntax

set spantree autoedge {**disable** | **enable**}

Parameters

disable | **enable**	Disables or enables automatic edge port detection.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to disable automatic edge port detection:

```
Matrix(rw)->set spantree autoedge disable
```

clear spantree autoedge

Use this command to reset automatic edge port detection to the default state of enabled.

Syntax

clear spantree autoedge

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to reset automatic edge port detection to enabled:

```
Matrix(rw)->clear spantree autoedge
```


Downloaded from www.Manualslib.com manuals search engine

show spantree legacypathcost

Use this command to display the default Spanning Tree path cost setting.

Syntax

```
show spantree legacypathcost
```

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Only.

Example

This example shows how to display the default Spanning Tree path cost setting:

```
Matrix(rw)->show spantree legacypathcost
Legacy Path Cost is disabled
```

set spantree legacypathcost

Use this command to enable or disable legacy (802.1D) path cost values.

Syntax

```
set spantree legacypathcost {disable | enable}
```

Parameters

disable | **enable**	Enables or disables legacy (802.1D) path cost values.

Defaults

None.

Mode

Switch command, Read-Write.

Usage

By default, legacy path cost is disabled. Enabling the device to calculate legacy path costs affects the range of valid values that can be entered in the **set spantree adminpathcost** command ("set spantree adminpathcost" on page 6-58).

Example

This example shows how to set the default path cost values to 802.1D:

```
Matrix(rw)->set spantree legacypathcost enable
```


Downloaded from www.Manualslib.com manuals search engine

clear spantree legacypathcost

Use this command to set the Spanning Tree default value for legacy path cost to 802.1t values.

Syntax

clear spantree legacypathcost

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to set the default path cost values to 802.1t:

```
Matrix(rw)->clear spantree legacypathcost
```

show spantree tctrapsuppress

Use this command to display the status of topology change trap suppression on Rapid Spanning Tree edge ports.

Syntax

show spantree tctrapsuppress

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Only.

Example

This example shows how to display the status of topology change trap suppression:

```
Matrix(rw)->show spantree tctrapsuppress
Topology change trap suppression is currently enabled.
```


Downloaded from www.Manualslib.com manuals search engine

set spantree tctrapsuppress

Use this command to disable or enable topology change trap suppression on Rapid Spanning Tree edge ports.

Syntax

```
set spantree tctrapsupress {disable | enable | edgedisable}
```

Parameters

disable | **enable**	Disables or enables topology change trap suppression.
edgedisable	Disables sending topology change traps on edge ports.

Defaults

None.

Mode

Switch command, Read-Write.

Usage

By default, RSTP non-edge (bridge) ports that transition to forwarding or blocking cause the switch to issue a topology change trap. When topology change trap suppression is enabled, which is the device default, edge ports (such as end station PCs) are prevented from sending topology change traps. This is because there is usually no need for network management to monitor edge port STP transition states, such as when PCs are powered on. When topology change trap suppression is disabled, all ports, including edge and bridge ports, will transmit topology change traps.

Example

This example shows how to allow Rapid Spanning Tree edge ports to transmit topology change traps:

```
Matrix(rw)->set spantree tctrapsuppress disable
```

clear spantree tctrapsuppress

Use this command to clear topology change trap suppression settings.

Syntax

```
clear spantree tctrapsuppress
```

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Write.

Downloaded from www.Manualslib.com manuals search engine

Example

This example shows how to clear topology change trap suppression settings:

```
Matrix(rw)->clear spantree tctrapsuppress
```

show spantree txholdcount

Use this command to display the maximum BPDU transmission rate.

Syntax

show spantree txholdcount

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Only.

Example

This example shows how to display the transmit hold count setting:

```
Matrix(rw)->show spantree txholdcount
Tx hold count = 3.
```

set spantree txholdcount

Use this command to set the maximum BPDU transmission rate.

Syntax

set spantree txholdcount *txholdcount*

Parameters

txholdcount	Specifies the maximum number of BPDUs to be transmitted before transmissions are subject to a one-second timer. Valid values are **1** - **10**. Default value is **6**.

Defaults

None.

Mode

Switch command, Read-Write.

Usage

Maximum BPDU transmission rate is the number of BPDUs which will be transmitted before transmissions are subject to a one-second timer.

Downloaded from www.Manualslib.com manuals search engine

Example

This example shows how to globally set the transmit hold count to 5:

```
Matrix(rw)->set spantree txholdcount 5
```

clear spantree txholdcount

Use this command to reset the transmit hold count to the default value of 6.

Syntax

clear spantree txholdcount

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to reset the transmit hold count:

```
Matrix(rw)->clear spantree txholdcount
```

show spantree maxhops

Use this command to display the Spanning Tree maximum hop count.

Syntax

show spantree maxhops

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Only.

Example

This example shows how to display the Spanning Tree maximum hop count:

```
Matrix(rw)->show spantree maxhops
Bridge Max Hop count is set to 20
```


Downloaded from www.Manualslib.com manuals search engine

set spantree maxhops

Use this command to set the Spanning Tree maximum hop count.

Syntax

set spantree maxhops *max_hop_count*

Parameters

max_hop_count	Specifies the maximum number of hops allowed. Valid values are **0** to **255**. Default value is **20**.

Defaults

None.

Mode

Switch command, Read-Write.

Usage

Spanning Tree maximum hop count is the maximum number of hops that the information for a particular Spanning Tree instance may traverse (via relay of BPDUs within the applicable MST region) before being discarded.

Example

This example shows how to set the maximum hop count to 40:

```
Matrix(rw)->set spantree maxhops 40
```

clear spantree maxhops

Use this command to reset the maximum hop count to the default value of 20.

Syntax

clear spantree maxhops

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to reset the maximum hop count to 20:

```
Matrix(rw)->clear spantree maxhops
```


Downloaded from www.Manualslib.com manuals search engine

show spantree spanguard

Use this command to display the status of the Spanning Tree span guard function.

Syntax

show spantree spanguard

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Only.

Example

This example shows how to display the span guard function status:

```
Matrix(rw)->show spantree spanguard
 spanguard is currently disabled.
```

set spantree spanguard

Use this command to enable or disable the Spanning Tree span guard function.

Syntax

set spantree spanguard {**enable** | **disable**}

Parameters

enable | **disable**	Enables or disables the span guard function.

Defaults

None.

Mode

Switch command, Read-Write.

Usage

When enabled, this prevents an unauthorized bridge from becoming part of the active Spanning Tree topology. It does this by disabling a port that receives a BPDU when that port has been defined as an edge (user) port (as described in "set spantree adminedge" on page 6-60). This port will remain disabled until the amount of time defined by the **set spantree spanguardtimeout** ("set spantree spanguardtimeout" on page 6-38) has passed since the last seen BPDU or the port is manually unlocked (as described in "clear / set spantree spanguardlock" on page 6-39).

Downloaded from www.Manualslib.com manuals search engine

Example

This example shows how to enable the span guard function:

```
Matrix(rw)->set spantree spanguard enable
```

clear spantree spanguard

Use this command to resets the status of the Spanning Tree span guard function to disabled.

Syntax

clear spantree spanguard

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to reset the status of the span guard function to disabled:

```
Matrix(rw)->clear spantree spanguard
```

show spantree spanguardtimeout

Use this command to display the Spanning Tree span guard timeout setting.

Syntax

show spantree spanguardtimeout

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Only.

Example

This example shows how to display the span guard timeout setting:

```
Matrix(rw)->show spantree spanguardtimeout
 spanguard timeout is set at 300 seconds.
```


Downloaded from www.Manualslib.com manuals search engine

set spantree spanguardtimeout

Use this command to set the amount of time (in seconds) an edge port will remain locked by the span guard function.

Syntax

set spantree spanguardtimeout *timeout*

Parameters

timeout	Specifies a timeout value in seconds. Valid values are **0** (forever) to **65535**.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to set the span guard timeout to 600 seconds:

```
Matrix(rw)->set spantree spanguardtimeout 600
```

clear spantree spanguardtimeout

Use this command to reset the Spanning Tree span guard timeout to the default value of 300 seconds.

Syntax

clear spantree spanguardtimeout

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to reset the span guard timeout to 300 seconds:

```
Matrix(rw)->clear spantree spanguardtimeout
```


Downloaded from www.Manualslib.com manuals search engine

show spantree spanguardlock

Use this command to display the span guard lock status of one or more ports.

Syntax

show spantree spanguardlock *port-string*

Parameters

port-string	Specifies the port(s) for which to show span guard lock status. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.

Defaults

None.

Mode

Switch command, Read-Only.

Example

This example shows how to display the span guard lock status for ge.2.1:

```
Matrix(rw)->show spantree spanguardlock ge.2.1
 spanguard status for port ge.2.1 is UNLOCKED.
```

clear / set spantree spanguardlock

Use either of these commands to unlock one or more ports locked by the Spanning Tree span guard function.

Syntax

clear spantree spanguardlock *port-string*

set spantree spanguardlock *port-string*

Parameters

port-string	Specifies port(s) to unlock. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.

Defaults

None.

Mode

Switch command, Read-Write.

Usage

When span guard is enabled, it locks ports that receive BPDUs when those ports have been defined as edge (user) ports (as described in "set spantree adminedge" on page 6-60).

Downloaded from www.Manualslib.com manuals search engine

Example

This example shows how to unlock port fe.1.16:

```
Matrix(rw)->clear spantree spanguardlock fe.1.16
```

show spantree spanguardtrapenable

Use this command to displays the state of the Spanning Tree span guard trap function.

Syntax

show spantree spanguardtrapenable

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Only.

Example

This example shows how to display the state of the span guard trap function:

```
Matrix(rw)->show spantree spanguardtrapenable
 Span Guard Trap is set to enable
```

set spantree spanguardtrapenable

Use this command to enable or disable the sending of an SNMP trap message when span guard detects that an unauthorized port has tried to join the Spanning Tree.

Syntax

set spantree spanguardtrapenable {**disable** | **enable**}

Parameters

disable | **enable**	Disables or enables the span guard trap function.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to disable the span guard trap function:

```
Matrix(rw)->set spantree spanguardtrapenable disable
```


Downloaded from www.Manualslib.com manuals search engine

clear spantree spanguardtrap enable

Use this command to reset the Spanning Tree span guard trap function back to the default state of enabled.

Syntax

clear spantree spanguardtrapenable

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to reset the span guard trap function to enabled:

```
Matrix(rw)->clear spantree spanguardtrapenable
```

show spantree backuproot

Use this command to display the state of the Spanning Tree backup root function.

Syntax

show spantree backuproot [*sid*]

Parameters

sid	(Optional) Displays status for a specific Spanning Tree. Valid values are **0** - **4094**. If not specified, SID 0 is assumed.

Defaults

If sid is not specified, status will be shown for Spanning Tree 0.

Mode

Switch command, Read-Only.

Example

This example shows how to display the status of the backup root function on SID 0:

```
Matrix(rw)->show spantree backuproot
Backup Root is set to disable on sid 0
```


Downloaded from www.Manualslib.com manuals search engine

set spantree backuproot

Use this command to enable or disable the Spanning Tree backup root function.

Syntax

set spantree backuproot *sid* {**enable** | **disable**}

Parameters

sid	Specifies the Spanning Tree on which to enable or disable the backup root function. Valid values are **0** - **4094**.
enable | **disable**	Enables or disables the backup root function.

Defaults

None.

Mode

Switch command, Read-Write.

Usage

Enabled by default on bridge(s) directly connected to the root bridge, this prevents stale Spanning Tree information from circulating in the event the root bridge is lost. If this happens, the backup root will dynamically lower its bridge priority so that it will be selected as the new root over the lost root bridge.

Example

This example shows how to enable the backup root function on SID 2:

```
Matrix(rw)->set spantree backuproot 2 enable
```

clear spantree backuproot

Use this command to reset the Spanning Tree backup root function to the default state of disabled.

Syntax

clear spantree backuproot *sid*

Parameters

sid	Specifies the Spanning Tree on which to reset the backup root function. Valid values are **0** - **4094**.

Defaults

None.

Mode

Switch command, Read-Write.

Downloaded from www.Manualslib.com manuals search engine

Example

This example shows how to reset the backup root function to disabled on SID 2:

```
Matrix(rw)->clear spantree backuproot 2
```

show spantree backuproottrapendable

Use this command to display the state of the Spanning Tree backup root trap function.

Syntax

show spantree backuproottrapenable

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Only.

Example

This example shows how to display the status of the backup root trap function:

```
Matrix(rw)->show spantree backuproottrapenable
Backup Root Trap is set to enable
```

set spantree backuproottrapenable

Use this command to enable or disable the Spanning Tree backup root trap function.

Syntax

set spantree backuproottrapenable {**enable** | **disable**}

Parameters

enable | **disable**	Enables or disables the backup root trap function.

Defaults

None.

Mode

Switch command, Read-Write.

Usage

When SNMP trap messageing is configured, this sends a trap message when the back up root function makes a Spanning Tree the new root of the network.

Downloaded from www.Manualslib.com manuals search engine

Example

This example shows how to enable the backup root trap function:

```
Matrix(rw)->set spantree backuproottrapenable enable
```

clear spantree backuproottrapenable

Use this command to resets the Spanning Tree backup root trap function to the default state of disabled.

Syntax

clear spantree backuproottrapenable.

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to reset the backup root trap function:

```
Matrix(rw)->clear spantree backuproottrapenable
```

show spantree newroottrapendable

Use this command to display the state of the Spanning Tree new root trap function.

Syntax

show spantree newroottrapenable

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Only.

Example

This example shows how to display the status of the new root trap function:

```
Matrix(rw)->show spantree newroottrapenable
New Root Trap is set to enable
```


Downloaded from www.Manualslib.com manuals search engine

set spantree newroottrapenable

Use this command to enable or disable the Spanning Tree new root trap function.

Syntax

```
set spantree newroottrapenable {enable | disable}
```

Parameters

enable | disable	Enables or disables the backup root trap function.

Defaults

None.

Mode

Switch command, Read-Write.

Usage

When SNMP trap messaging is configured, this sends a trap message when a Spanning Tree becomes the new root of the network.

Example

This example shows how to enable the new root trap function:

```
Matrix(rw)->set spantree newroottrapenable enable
```

clear spantree newroottrapenable

Use this command to reset the Spanning Tree new root trap function back to the default state of enabled.

Syntax

```
clear spantree newroottrapenable
```

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to reset the new root trap function to enabled:

```
Matrix(rw)->clear spantree newroottrapenable
```


Downloaded from www.Manualslib.com manuals search engine

clear spantree default

Use this command to restore default values to a Spanning Tree.

Syntax

clear spantree default [*sid*]

Parameters

sid	(Optional) Restores defaults on a specific Spanning Tree. Valid values are **0** - **4094**. If not specified, SID 0 is assumed.

Defaults

If *sid* is not specified, defaults will be restored on Spanning Tree 0.

Mode

Switch command, Read-Write.

Example

This example shows how to restore Spanning Tree defaults on SID 1:

```
Matrix(rw)->clear spantree default 1
```

show spantree debug

Use this command to display Spanning Tree debug counters for one or more ports.

Syntax

show spantree debug [**port** *port-string*] [sid *sid*] [**active**]

Parameters

port *port-string*	(Optional) Displays debug counters for specific port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.
sid *sid*	(Optional) Displays the debug counters for a specific Spanning Tree identifier. Valid values are **0** - **4094**. If not specified, SID 0 is assumed.
active	(Optional) Displays only the debug counters for ports that have received at least one configuration or RSTP BPDU.

Defaults

- If *port-string* is not specified, no port information will be displayed.
- If *sid* is not specified, debug counters will be displayed for Spanning Tree 0.

Mode

Switch command, Read-Only.

Downloaded from www.Manualslib.com manuals search engine

Example

This example shows how to display Spanning Tree debug counters for link aggregation port 3, SID 0:

```
Matrix(rw)->show spantree debug port lag.0.3

STP Diagnostic Common Counters for SID 0
----------------------------------------
Topology Change Count        - 379
Message Expiration Count     - 16
Invalid BPDU Count           - 0
STP BPDU Rx Count            - 3
STP BPDU Tx Count            - 3
STP TCN BPDU Rx Count        - 335
STP TCN BPDU Tx Count        - 0
STP TC BPDU Rx Count         - 0
STP TC BPDU Tx Count         - 0
RST BPDU Rx Count            - 81812
RST BPDU Tx Count            - 790319
RST TC BPDU Rx Count         - 2131
RST TC BPDU Tx Count         - 26623
MST BPDU Rx Count            - 0
MST BPDU Tx Count            - 0
MST CIST TC BPDU Rx Count    - 0
MST CIST TC BPDU Tx Count    - 0

STP Diagnostic Port Counters for Interface Number lag.0.3
---------------------------------------------------------
Port Role                    - RootPort
Message Expiration Count     - 4
Invalid BPDU Count           - 0
STP BPDU Rx Count            - 0
STP BPDU Tx Count            - 0
STP TCN BPDU Rx Count        - 0
STP TCN BPDU Tx Count        - 0
STP TC BPDU Rx Count         - 0
STP TC BPDU Tx Count         - 0
RST BPDU Rx Count            - 50263
RST BPDU Tx Count            - 47602
RST TC BPDU Rx Count         - 497
RST TC BPDU Tx Count         - 3325
MST BPDU Rx Count            - 0
MST BPDU Tx Count            - 0
MST CIST TC BPDU Rx Count    - 0
MST CIST TC BPDU Tx Count    - 0
```


Downloaded from www.Manualslib.com manuals search engine

clear spantree debug

Use this command to clear Spanning Tree debug counters.

Syntax

clear spantree debug

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to clear Spanning Tree debug counters:

```
Matrix(rw)->clear spantree debug
```


Downloaded from www.Manualslib.com manuals search engine

Configuring Spanning Tree Port Parameters

Purpose

To display and set Spanning Tree port parameters, including enabling or disabling the Spanning Tree algorithm on one or more ports, displaying designated bridge, port and root information, displaying blocked ports, displaying and setting Spanning Tree port priorities and costs, configuring edge port parameters, and setting point-to-point protocol mode.

Commands

For information about...	Refer to page...
show spantree portenable	6-50
set spantree portenable	6-50
clear spantree portenable	6-51
show spantree portadmin	6-51
set spantree portadmin	6-52
clear spantree portadmin	6-52
set spantree protomigration	6-53
show spantree portstate	6-53
show spantree blockedports	6-54
show spantree portpri	6-54
set spantree portpri	6-55
clear spantree portpri	6-56
set spantree porthello	6-56
clear spantree porthello	6-57
show spantree portcost	6-57
show spantree adminpathcost	6-58
set spantree adminpathcost	6-58
clear spantree adminpathcost	6-59
show spantree adminedge	6-60
set spantree adminedge	6-60
clear spantree adminedge	6-61
show spantree operedge	6-61
show spantree adminpoint	6-62
show spantree operpoint	6-62
set spantree adminpoint	6-63
clear spantree adminpoint	6-64

Downloaded from www.Manualslib.com manuals search engine

show spantree portenable

Use this command to display the port status on one or more Spanning Tree ports.

Syntax

show spantree portenable [**port** *port-string*]

Parameters

port *port-string*	(Optional) Displays status for specific port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.

Defaults

If *port-string* is not specified, status will be displayed for all ports.

Mode

Switch command, Read-Only.

Example

This example shows how to display status for port fe.1.12:

```
Matrix(rw)->show spantree portenable port fe.1.12
Port fe.1.12    has a Port Status of Enabled
```

set spantree portenable

Use this command to set the port status on one or more Spanning Tree ports.

Syntax

set spantree portenable *port-string* {**enable** | **disable**}

Parameters

port-string	Specifies the port(s) to enable or disable. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.
enable | **disable**	Enables or disables the Spanning Tree port.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to enable Spanning Tree port fe.1.12:

```
Matrix(rw)->set spantree portenable fe.1.12 enable
```


Downloaded from www.Manualslib.com manuals search engine

clear spantree portenable

Use this command to reset the default value for one or more Spanning Tree ports to enabled.

Syntax

clear spantree portenable *port-string*

Parameters

port-string	Specifies port(s) to reset. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to reset the default Spanning Tree port status value to enabled on fe.1.12:

```
Matrix(rw)->clear spantree portenable fe.1.12
```

show spantree portadmin

Use this command to display the status of the Spanning Tree algorithm on one or more ports.

Syntax

show spantree portadmin [**port** *port-string*]

Parameters

port *port-string*	(Optional) Displays status for specific port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.

Defaults

If *port-string* is not specified, status will be displayed for all ports.

Mode

Switch command, Read-Only.

Example

This example shows how to display port admin status for fe.1.7:

```
Matrix(rw)->show spantree portadmin port fe.1.7
Port fe.1.7 has portadmin set to enable
```


Downloaded from www.Manualslib.com manuals search engine

set spantree portadmin

Use this command to disable or enable the Spanning Tree algorithm on one or more ports.

Syntax

set spantree portadmin *port-string* {**disable** | **enable**}

Parameters

port-string	Specifies the port(s) for which to enable or disable Spanning Tree. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.
disable | **enable**	Disables or enables Spanning Tree.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to disable Spanning Tree on fe.1.5:

```
Matrix(rw)->set spantree portadmin fe.1.5 disable
```

clear spantree portadmin

Use this command to reset the default Spanning Tree admin status to enable on one or more ports.

Syntax

clear spantree portadmin *port-string*

Parameters

port-string	Resets the default admin status on specific port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to reset the default Spanning Tree admin state to enable on fe.1.12:

```
Matrix(rw)->clear spantree portadmin fe.1.12
```


Downloaded from www.Manualslib.com manuals search engine

set spantree protomigration

Use this command to reset the protocol state migration machine for one or more Spanning Tree ports. When operating in RSTP mode, this forces a port to transmit MSTP BPDUs.

Syntax

set spantree protomigration *port-string* **true**

Parameters

port-string	Specifies the port(s) for which protocol migration mode will be enabled. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.
true	Enables protocol migration mode.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to reset the protocol state migration machine on fe.1.12:

```
Matrix(rw)->set spantree protomigration fe.1.12 true
```

show spantree portstate

Use this command to display the state (blocking, forwarding, etc.) for a port on one or more Spanning Trees.

Syntax

show spantree portstate [**port** *port-string*] [**sid** *sid*]

Parameters

port *port-string*	(Optional) Displays the Spanning Tree state for specific Spanning Tree port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.
sid *sid*	(Optional) Displays the state for a specific Spanning Tree identifier. Valid values are **0** - **4094**. If not specified, SID 0 is assumed.

Defaults

- If *port-string* is not specified, current state will be displayed for all Spanning Tree ports.
- If *sid* is not specified, current port state will be displayed for Spanning Tree 0.

Mode

Switch command, Read-Only.

Downloaded from www.Manualslib.com manuals search engine

Example

This example shows how to display the Spanning Tree state for fe.1.7:

```
Matrix(rw)->show spantree portstate port fe.1.7
Port fe.1.7 has a Port State of Forwarding on SID 0
```

show spantree blockedports

Use this command to display the blocked ports in a Spanning Tree.

Syntax

show spantree blockedports [*sid*]

Parameters

sid	(Optional) Displays blocked ports on a specific Spanning Tree. Valid values are **0** - **4094**. If not specified, SID 0 is assumed.

Defaults

If *sid* is not specified, blocked ports will be displayed for Spanning Tree 0.

Mode

Switch command, Read-Only.

Usage

A port in this state does not participate in the transmission of frames, thus preventing duplication arising through multiple paths existing in the active topology of the bridged LAN. It receives Spanning Tree configuration messages, but does not forward packets.

Example

This example shows how to display blocked ports on SID 1:

```
Matrix(rw)->show spantree blockedports 1

SID   Port
---   ---------
1     fe.1.1
1     fe.1.3
1     fe.1.5

Number of blocked ports in SID 1 : 3
```

show spantree portpri

Use this command to show the Spanning Tree priority for one or more ports. Port priority is a component of the port ID, which is one element used in determining Spanning Tree port roles.

Syntax

show spantree portpri [**port** *port-string*] [**sid** *sid*]

Downloaded from www.Manualslib.com manuals search engine

Parameters

port *port-string*	(Optional) Specifies the port(s) for which to display Spanning Tree priority. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.
sid *sid*	(Optional) Displays port priority for a specific Spanning Tree identifier. Valid values are **0** - **4094**. If not specified, SID 0 is assumed.

Defaults

- If *port-string* is not specified, port priority will be displayed for all Spanning Tree ports.
- If *sid* is not specified, port priority will be displayed for Spanning Tree 0.

Mode

Switch command, Read-Only.

Example

This example shows how to display the port priority for fe.2.7:

```
Matrix(rw)->show spantree portpri port fe.2.7
Port fe.2.7 has a Port Priority of 128 on SID 0
```

set spantree portpri

Use this command to set a port's Spanning Tree priority.

Syntax

set spantree portpri *port-string priority* [**sid** *sid*]

Parameters

port-string	Specifies the port(s) for which to set Spanning Tree port priority. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.
priority	Specifies a number that represents the priority of a link in a Spanning Tree bridge. Valid values are from **0** to **240** (in increments of 16) with 0 indicating high priority.
sid *sid*	(Optional) Sets port priority for a specific Spanning Tree identifier. Valid values are **0** - **4094**. If not specified, SID 0 is assumed.

Defaults

If *sid* is not specified, port priority will be set for Spanning Tree 0.

Mode

Switch command, Read-Write.

Example

This example shows how to set the priority of fe.1.3 to 240 on SID 1.

```
Matrix(rw)->set spantree portpri fe.1.3 240 sid 1:
```


Downloaded from www.Manualslib.com manuals search engine

clear spantree portpri

Use this command to reset the bridge priority of a Spanning Tree port to a default value of 128.

Syntax

clear spantree portpri *port-string* [**sid** *sid*]

Parameters

port-string	Specifies the port(s) for which to set Spanning Tree port priority. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.
sid *sid*	(Optional) Resets the port priority for a specific Spanning Tree identifier. Valid values are **0** - **4094**. If not specified, SID 0 will be assumed.

Defaults

If *sid* is not specified, port priority will be set for Spanning Tree 0.

Mode

Switch command, Read-Write.

Example

This example shows how to reset the priority of fe.1.3 to 128 on SID 1:

```
Matrix(rw)->clear spantree portpri fe.1.3 sid 1:
```

set spantree porthello

Use this command to set the hello time for one or more Spanning Tree ports. This is the time interval (in seconds) the port(s) will transmit BPDUs.

Syntax

set spantree porthello *port-string interval*

Parameters

port-string	Specifies the port(s) for which to set hello time.
interval	Specifies the number of seconds the system waits before broadcasting a bridge hello message. Valid values are **1** - **10**.

Defaults

None.

Mode

Switch command, Read-Write.

Downloaded from www.Manualslib.com manuals search engine

Usage

This command can be executed only if bridge hello mode is disabled. For information on using the **set spantree bridgehellomode** command, refer to "set spantree bridgehellomode" on page 6-23.

Example

This example shows how to set the hello time to 3 seconds for port fe.1.4:

```
Matrix(rw)->set spantree porthello fe.1.4 3
```

clear spantree porthello

Use this command to reset the hello time for one or more Spanning Tree ports to the default of 2 seconds.

Syntax

clear spantree porthello *port-string*

Parameters

port-string	Specifies the port(s) for which to reset hello time.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to reset the hello time to 2 seconds for port fe.1.4:

```
Matrix(rw)->clear spantree porthello fe.1.4
```

show spantree portcost

Use this command to display cost values assigned to one or more Spanning Tree ports.

Syntax

show spantree portcost [**port** *port-string*] [**sid** *sid*]

Parameters

port *port-string*	(Optional) Displays cost values for specific port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.
sid s*id*	(Optional) Displays port cost for a specific Spanning Tree identifier. Valid values are **0** - **4094**. If not specified, SID 0 will be assumed.

Defaults

- If *port-string* is not specified, port cost will be displayed for all Spanning Tree ports.

Downloaded from www.Manualslib.com manuals search engine

- If *sid* is not specified, port cost will be displayed for all Spanning Trees.

Mode

Switch command, Read-Only.

Example

This example shows how to display the port cost for fe.2.5:

```
Matrix(rw)->show spantree portcost port fe.2.5
Port fe.2.5 has a Port Path Cost of 2000000 on SID 0
```

show spantree adminpathcost

Use this command to display the admin path cost for a port on one or more Spanning Trees.

Syntax

show spantree adminpathcost [**port** *port-string*] [**sid** *sid*]

Parameters

port *port-string*	(Optional) Displays the admin path cost value for specific port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.
sid *sid*	(Optional) Displays the admin path cost for a specific Spanning Tree identifier. Valid values are **0** - **4094**. If not specified, SID 0 will be assumed.

Defaults

- If *port-string* is not specified, admin path cost for all Spanning Tree ports will be displayed.
- If *sid* is not specified, admin path cost for Spanning Tree 0 will be displayed.

Mode

Switch command, Read-Only.

Example

This example shows how to display the admin path cost for fe.3.4 on SID 1:

```
Matrix(rw)->show spantree adminpathcost port fe.3.4 sid 1
Port fe.3.4 has a Port Admin Path Cost of 0 on SID 1
```

set spantree adminpathcost

Use this command to set the administrative path cost on a port and one or more Spanning Trees.

Syntax

set spantree adminpathcost *port-string cost* [**sid** *sid*]

Downloaded from www.Manualslib.com manuals search engine

Parameters

port-string	Specifies the port(s) on which to set an admin path cost. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.
cost	Specifies the port path cost. Va1id values are: • **0** - **65535** if legacy path cost is enabled. • **0** - **200000000** if legacy path cost is disabled.
sid *sid*	(Optional) Sets the admin path cost for a specific Spanning Tree identifier. Valid values are **0** - **4094**. If not specified, SID 0 will be assumed.

Defaults

If *sid* is not specified, admin path cost will be set for Spanning Tree 0.

Mode

Switch command, Read-Write.

Usage

By default, this value is set to 0, which forces the port to recalculate Spanning Tree path cost based on the speed of the port and whether or not legacy path cost is enabled. For details on using the **set spantree legacypathcost** command, refer to "set spantree legacypathcost" on page 6-30.

Example

This example shows how to set the admin path cost to 200 for fe.3.2 on SID 1:

```
Matrix(rw)->set spantree adminpathcost fe.3.2 200 sid 1
```

clear spantree adminpathcost

Use this command to reset the Spanning Tree default value for port admin path cost to 0.

Syntax

clear spantree adminpathcost *port-string* [**sid** *sid*]

Parameters

port-string	Specifies the port(s) for which to reset admin path cost. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.
sid *sid*	(Optional) Resets the admin path cost for specific Spanning Tree(s). Valid values are **0** - **4094**. If not specified, SID 0 is assumed.

Defaults

If *sid* is not specified, admin path cost will be reset for Spanning Tree 0.

Mode

Switch command, Read-Write.

Downloaded from www.Manualslib.com manuals search engine

Example

This example shows how to reset the admin path cost to 0 for fe.3.2 on SID 1:

```
Matrix(rw)->clear spantree adminpathcost fe.3.2 sid 1
```

show spantree adminedge

Use this command to display the edge port administrative status for a port.

Syntax

show spantree adminedge [**port** *port-string*]

Parameters

port-string	(Optional) Displays edge port administrative status for specific port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.

Defaults

If *port-string* is not specified edge port administrative status will be displayed for all Spanning Tree ports.

Mode

Switch command, Read-Only.

Example

This example shows how to display the edge port status for fe.3.2:

```
Matrix(rw)->show spantree adminedge port fe.3.2
Port fe.3.2 has a Port Admin Edge of Edge-Port
```

set spantree adminedge

Use this command to set the edge port administrative status on a Spanning Tree port.

Syntax

set spantree adminedge *port-string* {**true** | **false**}

Parameters

port-string	Specifies the edge port. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.
true | **false**	Enables (**true**) or disables (**false**) the specified port as a Spanning Tree edge port.

Defaults

None.

Downloaded from www.Manualslib.com manuals search engine

Mode

Switch command, Read-Write.

Example

This example shows how to set fe.1.11 as an edge port:

```
Matrix(rw)->set spantree adminedge fe.1.11 true
```

clear spantree adminedge

Use this command to reset a Spanning Tree port to non-edge status.

Syntax

clear spantree adminedge *port-string*

Parameters

port-string	Specifies port(s) on which to reset edge port status. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to reset fe.1.11 as a non-edge port:

```
Matrix(rw)->clear spantree adminedge fe.1.11
```

show spantree operedge

Use this command to display the Spanning Tree edge port operating status for a port.

Syntax

show spantree operedge [**port** *port-string*]

Parameters

port *port-string*	(Optional) Displays edge port operating status for specific port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.

Defaults

If *port-string* is not specified edge port operating status will be displayed for all Spanning Tree ports.

Downloaded from www.Manualslib.com manuals search engine

Mode

Switch command, Read-Only.

Example

This example shows how to display the edge port status for fe.2.7:

```
Matrix(rw)->show spantree operedge port fe.2.7
Port fe.2.7 has a Port Oper Edge of Edge-Port
```

show spantree adminpoint

Use this command to display the administrative point-to-point status of the LAN segment attached to a Spanning Tree port.

Syntax

show spantree adminpoint [**port** *port-string*]

Parameters

port *port-string*	(Optional) Displays point-to-point status for specific port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.

Defaults

If *port-string* is not specified, status will be displayed for all Spanning Tree port(s).

Mode

Switch command, Read-Only.

Example

This example shows how to display the point-to-point status of the LAN segment attached to fe.2.7:

```
Matrix(rw)->show spantree adminpoint port fe.2.7
Port fe.2.7 has a Port Admin Point to Point of Auto
```

show spantree operpoint

Use this command to display the operating point-to-point status of the LAN segment attached to a port.

Syntax

show spantree operpoint [**port** *port-string*]

Parameters

port *port-string*	(Optional) Displays point-to-point operating status for specific port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.

Downloaded from www.Manualslib.com manuals search engine

Defaults

If not specified, status will be displayed for all ports.

Mode

Switch command, Read-Only.

Example

This example shows how to display the point-to-point status operating of the LAN segment attached to fe.2.7:

```
Matrix(rw)->show spantree operpoint port fe.2.7
Port fe.2.7 has a Port Oper Point to Point of False on SID 1
```

set spantree adminpoint

Use this command to set the administrative point-to-point status of the LAN segment attached to a Spanning Tree port.

Syntax

set spantree adminpoint *port-string* {**true** | **false** | **auto**}

Parameters

port-string	Specifies the port on which to set point-to-point protocol status. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.
true | **false** | **auto**	Specifies the point-to-point status of the LAN attached to the specified port. • **true** forces the port to be considered point-to-point. • **false** forces the port to be considered non point-to-point. • **auto** (the default setting) allows the firmware to determine the port's point-to-point status.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to set the LAN attached to fe.1.3 as a point-to-point segment:

```
Matrix(rw)->set spantree adminpoint fe.1.3 true
```


Downloaded from www.Manualslib.com manuals search engine

clear spantree adminpoint

Use this command to reset the administrative point-to-point status of the LAN segment attached to a Spanning Tree port to auto mode.

Syntax

clear spantree adminpoint *port-string*

Parameters

port-string	Specifies port(s) on which to reset point-to-point protocol status. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to reset point-to-point status to auto on fe.2.3:

```
Matrix(rw)->clear spantree adminpoint fe.2.3
```


Downloaded from www.Manualslib.com manuals search engine

Configuring Spanning Tree Loop Protect Features

Purpose

To display and set Spanning Tree Loop Protect parameters, including the global parameters of Loop Protect threshold, window, enabling traps, and disputed BPDU threshold, as well as per port and port/SID parameters. See "Loop Protect" on page 2. for more information about the Loop Protect feature.

Commands

For information about...	Refer to page...
set spantree lp	6-65
show spantree lp	6-66
clear spantree lp	6-67
show spantree lplock	6-67
clear spantree lplock	6-68
set spantree lpcapablepartner	6-69
show spantree lpcapablepartner	6-70
clear spantree lpcapablepartner	6-70
set spantree lpthreshold	6-71
show spantree lpthreshold	6-71
clear spantree lpthreshold	6-72
set spantree lpwindow	6-72
show spantree lpwindow	6-73
clear spantree lpwindow	6-73
set spantree lptrapenable	6-74
show spantree lptrapenable	6-74
clear spantree lptrapenable	6-75
set spantree disputedbpduthreshold	6-75
show spantree disputedbpduthreshold	6-76
clear spantree disputedbpduthreshold	6-76
show spantree nonforwardingreason	6-77

set spantree lp

Use this command to enable or disable the Loop Protect feature per port and optionally, per SID.

Syntax

set spantree lp *port-string* {**enable** | **disable**} [**sid** *sid*]

Downloaded from www.Manualslib.com manuals search engine

Parameters

port-string	Specifies port(s) on which to enable or disable the Loop Protect feature. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.
enable | **disable**	Enables or disables the feature on the specified port.
sid *sid*	(Optional) Enables or disables the feature for specific Spanning Tree(s). Valid values are **0** - **4094**. If not specified, SID 0 is assumed.

Defaults

If no SID is specified, SID 0 is assumed.

Mode

Switch command, Read-Write.

Usage

The Loop Protect feature is disabled by default. See "Loop Protect" on page 2. for more information.

Loop Protect takes precedence over per port STP enable/disable (portAdmin). Normally portAdmin disabled would cause a port to go immediately to forwarding. If Loop Protect is enabled, that port should go to listening and remain there.

Note: The Loop Protect enable/disable settings for an MSTI port should match those for the CIST port.

Example

This example shows how to enable Loop Protect on fe.2.3:

```
Matrix(rw)->set spantree lp enable fe.2.3
```

show spantree lp

Use this command to display the Loop Protect status per port and/or per SID.

Syntax

show spantree lp [**port** *port-string*] [**sid** *sid*]

Parameters

port-string	(Optional) Specifies port(s) for which to display the Loop Protect feature status. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.
sid *sid*	(Optional) Specifies the specific Spanning Tree(s) for which to display the Loop Protect feature status. Valid values are **0** - **4094**. If not specified, SID 0 is assumed.

Defaults

If no *port-string* is specified, status is displayed for all ports.

Downloaded from www.Manualslib.com manuals search engine

If no SID is specified, SID 0 is assumed.

Mode

Switch command, Read-Only.

Example

This example shows how to display Loop Protect status on fe.2.3:

```
Matrix(rw)->show spantree lp port fe.2.3
LoopProtect is enabled on port fe.2.3    , SID 0
```

clear spantree lp

Use this command to return the Loop Protect status per port and optionally, per SID, to its default state of disabled.

Syntax

clear spantree lp *port-string* [**sid** *sid*]

Parameters

port-string	Specifies port(s) for which to clear the Loop Protect feature status. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.
sid *sid*	(Optional) Specifies the specific Spanning Tree(s) for which to clear the Loop Protect feature status. Valid values are **0** - **4094**. If not specified, SID 0 is assumed.

Defaults

If no SID is specified, SID 0 is assumed.

Mode

Switch command, Read-Write.

Example

This example shows how to return the Loop Protect state on fe.2.3 to disabled:

```
Matrix(rw)->clear spantree lp port fe.2.3
```

show spantree lplock

Use this command to display the Loop Protect lock status per port and/or per SID.

Syntax

show spantree lplock [**port** *port-string*] [**sid** *sid*]

Downloaded from www.Manualslib.com manuals search engine

Parameters

port-string	(Optional) Specifies port(s) for which to display the Loop Protect lock status. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.
sid *sid*	(Optional) Specifies the specific Spanning Tree(s) for which to display the Loop Protect lock status. Valid values are **0** - **4094**. If not specified, SID 0 is assumed.

Defaults

If no *port-string* is specified, status is displayed for all ports.

If no SID is specified, SID 0 is assumed.

Mode

Switch command, Read-Only.

Usage

A port can become locked if a configured number of Loop Protect events occur during the configured window of time. See the set spantree lpthreshold and set spantree lpwindow commands. Once a port is forced into blocking (locked), it remains locked until manually unlocked with the clear spantree lplock command.

Example

This example shows how to display Loop Protect lock status on ge.1.1:

```
Matrix(rw)->show spantree lplock port ge.1.1
LoopProtect Lock status for port ge.1.1    , SID 0   is UNLOCKED.
```

clear spantree lplock

Use this command to manually unlock a blocked port and optionally, per SID.

Syntax

clear spantree lplock *port-string* [**sid** *sid*]

Parameters

port-string	Specifies port(s) for which to clear the Loop Protect lock. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.
sid *sid*	(Optional) Specifies the specific Spanning Tree(s) for which to clear the Loop Protect lock. Valid values are **0** - **4094**. If not specified, SID 0 is assumed.

Defaults

If no SID is specified, SID 0 is assumed.

Mode

Switch command, Read-Only.

Downloaded from www.Manualslib.com manuals search engine

Usage

The default state is unlocked.

Example

This example shows how to clear Loop Protect lock from ge.1.1:

```
Matrix(rw)->show spantree lplock port ge.1.1
LoopProtect Lock status for port ge.1.1    , SID 0   is LOCKED.
Matrix(rw)->clear spantree lplock ge.1.1
Matrix(rw)->show spantree lplock port ge.1.1
LoopProtect Lock status for port ge.1.1    , SID 0   is UNLOCKED.
```

set spantree lpcapablepartner

Use this command to specify per port whether the link partner is Loop Protect capable.

Syntax

set spantree lpcapablepartner *port-string* {**true** | **false**}

Parameters

port-string	Specifies port(s) for which to configure a Loop Protect capable link partner. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.
true | **false**	Specifies whether the link partner is capable (true) or not (false).

Defaults

None.

Mode

Switch command, Read-Write.

Usage

The default value for Loop Protect capable partner is false. If the port is configured with a Loop Protect capable partner (true), then the full functionality of the Loop Protect feature is used. If the value is false, then there is some ambiguity as to whether an Active Partner timeout is due to a loop protection event or is a normal situation due to the fact that the partner port does not transmit Alternate Agreement BPDUs. Therefore, a conservative approach is taken in that designated ports will not be allowed to forward unless receiving agreements from a port with root role.

This type of timeout will not be considered a loop protection event. Loop protection is maintained by keeping the port from forwarding but since this is not considered a loop event it will not be factored into locking the port.

See "Loop Protect" on page 2. for more information.

Example

This example shows how to set the Loop Protect capable partner to true for ge.1.1:

```
Matrix(rw)->set spantree lpcapablepartner ge.1.1 true
```


Downloaded from www.Manualslib.com manuals search engine

show spantree lpcapablepartner

Use this command to the Loop Protect capability of a link partner for one or more ports.

Syntax

show spantree lpcapablepartner [**port** *port-string*]

Parameters

port-string	(Optional) Specifies port(s) for which to display Loop Protect capability for its link partner. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.

Defaults

If no *port-string* is specified, Loop Protect capability for link partners is displayed for all ports.

Mode

Switch command, Read-Only.

Example

This example shows how to display the Loop Protect partner capability for ge.1.1:

```
Matrix(rw)->show spantree lpcapablepartner port ge.1.1
Link partner of port ge.1.1     is not LoopProtect-capable.
```

clear spantree lpcapablepartner

Use this command to reset the Loop Protect capability of port link partners to the default state of false.

Syntax

clear spantree lpcapablepartner *port-string*

Parameters

port-string	Specifies port(s) for which to clear their link partners' Loop Protect capability (reset to false). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to reset the Loop Protect partner capability for ge.1.1:

```
Matrix(rw)->clear spantree lpcapablepartner ge.1.1
```


Downloaded from www.Manualslib.com manuals search engine

set spantree lpthreshold

Use this command to set the Loop Protect event threshold.

Syntax

set spantree lpthreshold *value*

Parameters

value	Specifies the number of events that must occur during the event window in order to lock a port/SID. The default value is 3 events. A threshold of 0 specifies that ports will never be locked.

Defaults

None. The default event threshold is 3.

Mode

Switch command, Read-Write.

Usage

The LoopProtect event threshold is a global integer variable that provides protection in the case of intermittent failures. The default value is 3. If the event counter reaches the threshold within a given period (the event window), then the port, for the given SID, becomes locked (that is, held indefinitely in the blocking state). If the threshold is 0, the ports are never locked.

Example

This example shows how to set the Loop Protect threshold value to 4:

```
Matrix(rw)->set spantree lpthreshold 4
```

show spantree lpthreshold

Use this command to display the current value of the Loop Protect event threshold.

Syntax

show spantree lpthreshold

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Only.

Downloaded from www.Manualslib.com manuals search engine

Example

This example shows how to display the current Loop Protect threshold value:

```
Matrix(rw)->show spantree lpthreshold
LoopProtect event threshold is set to 4
```

clear spantree lpthreshold

Use this command to return the Loop Protect event threshold to its default value of 3.

Syntax

clear spantree lpthreshold

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to reset the Loop Protect event threshold to the default of 3:

```
Matrix(rw)->clear spantree lpthreshold
```

set spantree lpwindow

Use this command to set the Loop Protect event window value in seconds.

Syntax

set spantree lpwindow *value*

Parameters

value	Specifies the number of seconds that comprise the period during which Loop Protect events are counted. The default event window is 180 seconds.

Defaults

None.

Mode

Switch command, Read-Write.

Usage

The Loop Protect Window is a timer value, in seconds, that defines a period during which Loop Protect events are counted. The default value is 180 seconds. If the timer is set to 0, the event

Downloaded from www.Manualslib.com manuals search engine

counter is not reset until the Loop Protect event threshold is reached. If the threshold is reached, that constitutes a loop protection event.

Example

This example shows how to set the Loop Protect event window to 120 seconds:

```
Matrix(rw)->set spantree lpwindow 120
```

show spantree lpwindow

Use this command to display the current Loop Protect event window value.

Syntax

show spantree lpwindow

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Only.

Example

This example shows how to display the current Loop Protect window value:

```
Matrix(rw)->show spantree lpwindow
LoopProtect event window is set to 120 seconds
```

clear spantree lpwindow

Use this command to reset the Loop Protect event window to the default value of 180 seconds.

Syntax

clear spantree lpwindow

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Write.

Downloaded from www.Manualslib.com manuals search engine

Example

This example shows how to reset the Loop Protect event window to the default of 180 seconds:

```
Matrix(rw)->clear spantree lpwindow
```

set spantree lptrapenable

Use this command to enable or disable Loop Protect event notification.

Syntax

set spantree lptrapenable {**enable** | **disable**}

Parameters

enable | **disable**	Enables or disables the sending of Loop Protect traps. Default is disabled.

Defaults

None.

Mode

Switch command, Read-Write.

Usage

Loop Protect traps are sent when a Loop Protect event occurs, that is, when a port goes to listening due to not receiving BPDUs. The trap indicates port, SID and loop protection status.

Example

This example shows how to enable sending of Loop Protect traps:

```
Matrix(rw)->set spantree lptrapenable enable
```

show spantree lptrapenable

Use this command to display the current status of Loop Protect event notification.

Syntax

show spantree lptrapenable

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Only.

Downloaded from www.Manualslib.com manuals search engine

Example

This example shows how to display the current Loop Protect event notification status:

```
Matrix(rw)->show spantree lptrapenable
LoopProtect event traps are enabled
```

clear spantree lptrapenable

Use this command to return the Loop Protect event notification state to its default state of disabled.

Syntax

clear spantree lptrapenable

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to reset the Loop Protect event notification state to the default of disabled

```
Matrix(rw)->clear spantree lptrapenable
```

set spantree disputedbpduthreshold

Use this command to set the disputed BPDU threshold, which is the number of disputed BPDUs that must be received on a given port/SID until a disputed BPDU trap is sent.

Syntax

set spantree disputedbpduthreshold *value*

Parameters

value	Specifies the number of disputed BPDUs that must be received on a given port/SID to cause a disputed BPDU trap to be sent. A threshold of 0 indicates that traps should not be sent. The default value is 0.

Defaults

None.

Mode

Switch command, Read-Write.

Downloaded from www.Manualslib.com manuals search engine

Usage

A disputed BPDU is one in which the flags field indicates a designated role and learning, and the priority vector is worse than that already held by the port. If a disputed BPDU is received the port is forced to the listening state. Refer to the 802.1Q-2005 standard, *IEEE Standard for Local and Metropolitan Area Networks – Virtual Bridged Local Area Networks*, for a full description of the dispute mechanism, which prevents looping in cases of one-way communication.

The disputed BPDU threshold is an integer variable that represents the number of disputed BPDUs that must be received on a given port/SID until a disputed BPDU trap is sent and a syslog message is issued. For example, if the threshold is 10, then a trap is issued when 10, 20, 30, and so on, disputed BPDUs have been received.

If the value is 0, traps are not sent. The trap indicates port, SID and total Disputed BPDU count. The default is 0.

Example

This example shows how to set the disputed BPDU threshold value to 5:

```
Matrix(rw)->set spantree disputedbpduthreshold 5
```

show spantree disputedbpduthreshold

Use this command to display the current value of the disputed BPDU threshold.

Syntax

show spantree disputedbpduthreshold

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Only.

Example

This example shows how to display the current disputed BPDU threshold:

```
Matrix(rw)->show spantree disputedbpduthreshold
Disputed BPDU threshold is set to 0
```

clear spantree disputedbpduthreshold

Use this command to return the disputed BPDU threshold to its default value of 0, meaning that disputed BPDU traps should not be sent.

Syntax

clear spantree disputedbpduthreshold

Downloaded from www.Manualslib.com manuals search engine

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to reset the disputed BPDU threshold to the default of 0:

```
Matrix(rw)->clear spantree disputedbpduthreshold
```

show spantree nonforwardingreason

Use this command to display the reason for placing a port in a non-forwarding state due to an exceptional condition.

Syntax

show spantree nonforwardingreason [**port** *port-string*] [**sid** *sid*]

Parameters

port-string	(Optional) Specifies port(s) for which to display the non-forwarding reason. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.
sid *sid*	(Optional) Specifies the specific Spanning Tree(s) for which to display the non-forwarding reason. Valid values are **0** - **4094**. If not specified, SID 0 is assumed.

Defaults

If no *port-string* is specified, non-forwarding reason is displayed for all ports.

If no SID is specified, SID 0 is assumed.

Mode

Switch command, Read-Only.

Usage

Exceptional conditions causing a port to be placed in listening or blocking state include a Loop Protect event, receipt of disputed BPDUs, and loopback detection.

Example

This example shows how to display the non-forwarding reason on ge.1.1:

```
Matrix(rw)->show spantree nonforwardingreason port ge.1.1
Port ge.1.1 has not been placed in a non-forwarding state on SID 0 due to any
exceptional condition.
```


Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

7

802.1Q VLAN Configuration

This chapter describes the Enterasys Matrix system's capabilities to implement 802.1Q virtual LANs (VLANs). It documents how to:

- Create, enable, disable and name a VLAN.
- Review status and other information related to VLANs.
- Assign ports to a VLAN and filter unwanted frames on one or more ports
- Assign a VLAN to a MIB-II interface in order to view statistics for the VLAN
- Use GVRP (GARP VLAN Registration Protocol) to control and propagate VLAN knowledge through the network.
- Create a secure VLAN for device management security.

Note: The device can support up to 4094 802.1Q VLANs. The allowable range for VLANs is 2 to 4094. As a default, all ports on the device are assigned to VLAN ID 1, untagged.

For information about...	Refer to page...
VLAN Configuration Summary	7-1
Reviewing Existing VLANs	7-3
Creating and Naming Static VLANs	7-6
Assigning Port VLAN IDs (PVIDs) and Ingress Filtering	7-9
Configuring the VLAN Egress List	7-17
Enabling/Disabling GVRP	7-22

VLAN Configuration Summary

Virtual LANs allow the network administrator to partition network traffic into logical groups and control the flow of that traffic through the network. Once the traffic and, in effect, the users creating the traffic, are assigned to a VLAN, then broadcast and multicast traffic is contained within the VLAN and users can be allowed or denied access to any of the network's resources. Also, some or all of the ports on the device can be configured as GVRP ports, which enable frames received with a particular VLAN ID and protocol to be transmitted on a limited number of ports. This keeps the traffic associated with a particular VLAN and protocol isolated from the other parts of the network.

Downloaded from www.Manualslib.com manuals search engine

Port Assignment Scheme

For information on this device's port assignment scheme, refer to "Port String Syntax Used in the CLI" on page 4-2.

Port String Syntax Used in the CLI

For information on how to designate port numbers in the CLI syntax, refer to "Port String Syntax Used in the CLI" on page 4-2.

Preparing for VLAN Configuration

A little forethought and planning is essential to a good VLAN implementation. Before attempting to configure a single device for VLAN operation, consider the following:

- How many VLANs will be required?
- What stations will belong to them?
- What ports are connected to those stations?
- What ports will be configured as GVRP-aware ports?

It is also helpful to sketch out a diagram of your VLAN strategy.

About PVIDs and Policy Classification to a VLAN

Port VLAN IDs (PVIDs) assign VLAN IDs to untagged frames on one or more ports. Using the **set port vlan** command as described in "set port vlan" on page 7-10, you can, for example, assign ports 1, 5, 8, and 9 to VLAN 3. Untagged frames received on those ports will be assigned to VLAN 3. (By default, all ports are members of VLAN ID 1, the default VLAN.)

Policy classification to a VLAN, as described in Chapter 8, "set policy rule" on page 8-13, takes precedence over PVID assignment if:

- Policy classification is configured to a VLAN as described in "set policy rule" on page 8-13, and
- PVID override has been enabled for a policy profile, and assigned to port(s) associated with the PVID as described in "set policy profile" on page 8-3.

For more information about configuring user policy profiles, including PVID override, protocol-based policy classification a VLAN or Class of Service, and assigning ports to policy profiles, refer to Chapter 8.

Creating a Secure Management VLAN

If the Matrix Series device is to be configured for multiple VLAN's, it may be desirable to configure a management-only VLAN. This allows a station connected to the management VLAN to manage the device. It also makes management secure by preventing configuration via ports assigned to other VLANs.

To create a secure management VLAN, you must:

1. Create a new VLAN. ("set vlan" on page 7-6)
2. Set the PVID for the host port and the desired switch port to the VLAN created in Step 1. ("set port vlan" on page 7-10)

Downloaded from www.Manualslib.com manuals search engine

3. Add the host port and the desired switch port to the egress list for the VLAN created in Step 1. (“set vlan egress” on page 7-18)
4. Set a private community name and access policy. (“set snmp community” on page 5-16)

The commands used to create a secure management VLAN are listed in Table 7-1 and described in the associated sections as shown. This example assumes the management station is attached to fe.1.1 and wants untagged frames.The process described in this section would be repeated on every device that is connected in the network to ensure that each device has a secure management VLAN.

Note: By default at device startup, there is one VLAN configured on the Matrix Series device. It is VLAN ID 1, the DEFAULT VLAN. The default community name, which determines remote access for SNMP management, is set to “public” with read-write access.

Table 7-1 Command Set for Creating a Secure Management VLAN

To do this...	Use these commands...
Create a new VLAN and confirm settings.	**set vlan create 2** (“set vlan” on page 7-6)
	(Optional) **show vlan 2** (“show vlan” on page 7-3)
Set the PVIDs to the new VLAN.	**set port vlan host.0.1; fe.1.1 2** (“set port vlan” on page 7-10)
Add the ports to the new VLAN’s egress list.	**set vlan egress 2 host.0.1; fe.1.1 2 untagged** (“set vlan egress” on page 7-18)
Set a private community name and access policy and confirm settings.	**set snmp community private** (“set snmp community” on page 5-16)
	(Optional) **show snmp community** (“show snmp community” on page 5-15)

Reviewing Existing VLANs

Purpose

To display a list of VLANs currently configured on the device, to determine how one or more VLANs were created, the ports allowed and disallowed to transmit traffic belonging to VLAN(s), and if those ports will transmit the traffic with a VLAN tag included.

Command

For information about...	Refer to page...
show vlan	7-3

show vlan

Use this command to display all information related to one or more VLANs.

Syntax

show vlan [**static**] [*vlan-list*]

Downloaded from www.Manualslib.com manuals search engine

Parameters

static	(Optional) Displays information related to static VLANs. Static VLANs are manually created using the **set vlan** command ("set vlan" on page 7-6), SNMP MIBs, or the WebView management application. The default VLAN, VLAN 1, is always statically configured and can't be deleted. Only ports that use a specified VLAN as their default VLAN (PVID) will be displayed.
vlan-list	(Optional) Displays information for a specific VLAN or range of VLANs.

Defaults

If no options are specified, all information related to static and dynamic VLANs will be displayed.

Mode

Switch command, Read-Only.

Example

This example shows how to display information for VLAN 1. In this case, VLAN 1 is named "DEFAULT VLAN" and it is enabled to operate. Ports allowed to transmit frames belonging to VLAN 1 are listed as egress ports. Ports that won't include a VLAN tag in their transmitted frames are listed as untagged ports. There are no forbidden ports (prevented from transmitted frames) on VLAN 1:

```
Matrix(rw)->show vlan 1
 VLAN: 1         NAME: DEFAULT VLAN                      Status: Enabled
 VLAN Type: Permanent    FID: 1
 Creation Time: 4 days 9 hours 4 minutes 50 seconds ago
 Egress Ports
host.0.1, fe.1.1-10, ge.2.1-4, fe.3.1-7, lag.0.1-32
 Forbidden Egress Ports
None.
 Untagged Ports
host.0.1, fe.1.1-10, ge.2.1-4, fe.3.1-7, lag.0.1-32
```

Table 7-2 provides an explanation of the command output.

Table 7-2 show vlan Output Details

Output...	What it displays...
VLAN	VLAN ID.
NAME	Name assigned to the VLAN.
Status	Whether it is **enabled** or **disabled**.
VLAN Type	Whether it is **permanent** (static) or **dynamic**.
FID	Filter Database ID of which this VLAN is a member.
Creation Time	Time elapsed since the VLAN was created.
Egress Ports	Ports configured to transmit frames for this VLAN.

Downloaded from www.Manualslib.com manuals search engine

Table 7-2 show vlan Output Details (continued)

Output...	What it displays...
Forbidden Egress Ports	Ports prevented from transmitted frames for this VLAN.
Untagged Ports	Ports configured to transmit untagged frames for this VLAN.

Downloaded from www.Manualslib.com manuals search engine

Creating and Naming Static VLANs

Purpose

To create a new static VLAN, or to enable or disable existing VLAN(s).

Commands

For information about...	Refer to page...
set vlan	7-6
set vlan name	7-7
clear vlan	7-7
clear vlan name	7-8

set vlan

Use this command to create a new static IEEE 802.1Q VLAN, or to enable or disable an existing VLAN.

Syntax

set vlan {**create** | **enable** | **disable**} *vlan-list*

Parameters

create | **enable** | **disable**	Creates, enables or disables VLAN(s).
vlan-list	Specifies one or more VLAN IDs to be created, enabled or disabled.

Defaults

None.

Mode

Switch command, Read-Write.

Usage

Each VLAN ID must be unique. If a duplicate VLAN ID is entered, the device assumes that the Administrator intends to modify the existing VLAN.

Enter the VLAN ID using a unique number between 2 and 4094. The VLAN IDs of 0, 1, and 4094 and higher may not be used for user-defined VLANs.

Once a VLAN is created, you can assign it a name using the **set vlan name** command described in "set vlan name" on page 7-7.

Downloaded from www.Manualslib.com manuals search engine

Examples

This example shows how to create VLAN 3:

```
Matrix(rw)->set vlan create 3
```

This example shows how to disable VLAN 3:

```
Matrix(rw)->set vlan disable 3
```

set vlan name

Use this command to set or change the ASCII name for a new or existing VLAN.

Syntax

set vlan name *vlan-list vlan-name*

Parameters

vlan-list	Specifies the VLAN ID of the VLAN(s) to be named.
vlan-name	Specifies the string used as the name of the VLAN (1 to 32 characters).

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to set the name for VLAN 7 to green:

```
Matrix(rw)->set vlan name 7 green
```

clear vlan

Use this command to remove a static VLAN from the list of VLANs recognized by the device.

Syntax

clear vlan *vlan-list*

Parameters

vlan-list	Specifies the VLAN ID of the VLAN(s) to be removed.

Defaults

None.

Mode

Switch command, Read-Write.

Downloaded from www.Manualslib.com manuals search engine

Example

This example shows how to remove a static VLAN 9 from the device's VLAN list:

```
Matrix(rw)->clear vlan 9
```

clear vlan name

Use this command to remove the name of a VLAN from the VLAN list.

Syntax

clear vlan name *vlan-list*

Parameters

vlan-list	Specifies the VLAN ID of the VLAN(s) for which the name will be cleared.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to clear the name for VLAN 9:

```
Matrix(rw)->clear vlan name 9
```


Downloaded from www.Manualslib.com manuals search engine

Assigning Port VLAN IDs (PVIDs) and Ingress Filtering

Purpose

To assign default VLAN IDs to untagged frames on one or more ports, to configure MIB-II interface mapping to a VLAN, to configure VLAN ingress filtering, and to set the frame discard mode.

Commands

For information about...	Refer to page...
show port vlan	7-9
set port vlan	7-10
clear port vlan	7-11
show vlan interface	7-11
set vlan interface	7-12
clear vlan interface	7-13
show port ingress filter	7-13
set port ingress filter	7-14
show port discard	7-15
set port discard	7-15
clear port discard	7-16

show port vlan

Use this command to display port VLAN identifier (PVID) information.

Syntax

show port vlan [*port-string*]

Parameters

port-string	(Optional) Displays PVID information for specific port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.

Defaults

If *port -string* is not specified, port VLAN information for all ports will be displayed.

Mode

Switch command, Read-Only.

Downloaded from www.Manualslib.com manuals search engine

Usage

PVID determines the VLAN to which all untagged frames received on one or more ports will be classified.

Example

This example shows how to display PVIDs assigned to Fast Ethernet ports 1 through 6 in module 2. In this case, untagged frames received on these ports will be classified to VLAN 1:

```
Matrix(rw)->show port vlan fe.2.1-6
fe.2.1 is set to 1
fe.2.2 is set to 1
fe.2.3 is set to 1
fe.2.4 is set to 1
fe.2.5 is set to 1
fe.2.6 is set to 1
```

set port vlan

Use this command to configure the PVID (port VLAN identifier) for one or more ports.

Syntax

`set port vlan` *port-string pvid* [**`modify-egress`** | **no-modify-egress**]

Parameters

port-string	Specifies the port(s) for which to configure a VLAN identifier. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.
pvid	Specifies the VLAN ID of the VLAN to which port(s) will be added.
modify-egress | **no-modify-egress**	(Optional) Adds port(s) to VLAN's untagged egress list and removes them from other untagged egress lists, or does not prompt for or make egress list changes

Defaults

If not specified, the egress list will be modified.

Mode

Switch command, Read-Write.

Usage

For information on how to configure protocol-based policy classification to a VLAN, including how to configure a VLAN policy to override PVID, refer to Chapter 8.

The PVID is used to classify untagged frames as they ingress into a given port. If the specified VLAN has not already been created, this command will create it. It will prompt the user to add the VLAN to the port's egress list as untagged, and remove the default VLAN from the port's egress list.

Downloaded from www.Manualslib.com manuals search engine

Example

This example shows how to add fe.1.10 to the port VLAN list of VLAN 4 (PVID 4). Since VLAN 4 is a new VLAN, it is created. Then port fe.1.10 is added to VLAN 4's untagged egress list, and is cleared from the egress list of VLAN 1 (the default VLAN):

```
Matrix(rw)->set port vlan fe.1.10 4
Matrix(rw)->set vlan 4 create
Matrix(rw)->set vlan egress 4 fe.1.10 untagged
Matrix(rw)->clear vlan egress 1 fe.1.10
```

clear port vlan

Use this command to reset a port's 802.1Q port VLAN ID (PVID) to the host VLAN ID 1.

Syntax

clear port vlan *port-string*

Parameters

port-string	Specifies the port(s) to be reset to the host VLAN ID 1. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to reset the Fast Ethernet ports 3 and 11 in module1 to a VLAN ID of 1 (Host VLAN):

```
Matrix(rw)->clear port vlan fe.1.3,fe.1.11
```

show vlan interface

Use this command to display the MIB-II interface entry mapped to a VLAN.

Syntax

show vlan interface [*vlan-list*]

Parameters

vlan-list	(Optional) Displays the MIB2 interface entry for specific VLAN(s).

Defaults

If *vlan-list* is not specified, MIB2 interface entries will be displayed for all VLANs.

Downloaded from www.Manualslib.com manuals search engine

Mode

Switch command, Read-Only.

Example

This example shows how to display the interface entry for VLAN 1:

```
Matrix(rw)->show vlan interface 1
VLAN       Port          Storage Type
-------------------------------------
  1      vlan.0.1        non-volatile
```

Table 7-3 provides an explanation of the command output.

Table 7-3 show vlan interface Output Details

Output...	What it displays...
VLAN	VLAN ID.
Port	Port-string designation.
Storage Type	Whether the entry is stored as a **volatile** or **non-volatile** entry. Volatile entries are lost when a system is reset. Non-volatile entries are saved in NVRAM and are persistent until cleared.

set vlan interface

Use this command to create, disable or enables a MIB-II interface mapped to a VLAN.

Syntax

set vlan interface *vlan-list* {**create** | **disable** | **enable**} [**volatile**]

Parameters

vlan-list	Specifies the VLAN(s) for which an interface entry will be created, disabled or enabled.
create | **disable** | **enable**	Creates, disables or enables an interface entry.
volatile	(Optional) When the **create** keyword is used, stores the entry as a volatile entry. Volatile entries are lost when a system is reset. Non-volatile entries are saved in NVRAM and are persistent until cleared.

Defaults

If **volatile** is not specified, entries will be created as nonvolatile.

Mode

Switch command, Read-Write.

Example

This example shows how to create a volatile interface entry mapped to VLAN 1:

```
Matrix(rw)->set vlan interface 1 volatile
```


Downloaded from www.Manualslib.com manuals search engine

clear vlan interface

Use this command to clear the MIB-II interface entry mapped to a VLAN.

Syntax

clear vlan interface *vlan-list*

Parameters

vlan-list	Specifies the VLAN(s) for which an interface entry will be cleared.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to clear the interface entry mapped to VLAN 1:

```
Matrix(rw)->clear vlan interface 1
```

show port ingress filter

Use this command to show all ports that are enabled for port ingress filtering, which limits incoming VLAN ID frames according to a port VLAN egress list.

Syntax

show port ingress-filter [*port-string*]

Parameters

port-string	(Optional) Specifies the port(s) for which to display ingress filtering status. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.

Defaults

If *port-string* is not specified, ingress filtering status for all ports will be displayed.

Mode

Switch command, Read-Only.

Usage

If the VLAN ID specified in the received frame is not on the port's VLAN egress list, then that frame is dropped and not forwarded.

Downloaded from www.Manualslib.com manuals search engine

Example

This example shows how to display the port ingress filter status for Fast Ethernet ports 10 through 15 in module 1. In this case, the ports are disabled for ingress filtering:

```
Matrix(rw)->show port ingress-filter fe.1.10-15
   Port      State
 --------  ---------
  fe.1.10  disabled
  fe.1.11  disabled
  fe.1.12  disabled
  fe.1.13  disabled
  fe.1.14  disabled
  fe.1.15  disabled
```

set port ingress filter

Use this command to discard all frames received with a VLAN ID that don't match the port's VLAN egress list.

Syntax

set port ingress-filter *port-string* {disable | enable}

Parameters

port-string	Specifies the port(s) on which to enable of disable ingress filtering. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.
disable | **enable**	Disables or enables ingress filtering.

Defaults

None.

Mode

Switch command, Read-Write.

Usage

When ingress filtering is enabled on a port, the VLAN IDs of incoming frames are compared to the port's egress list. If the received VLAN ID does not match a VLAN ID on the port's egress list, then the frame is dropped.

Ingress filtering is implemented according to the IEEE 802.1Q standard.

Example

This example shows how to enable port ingress filtering on Fast Ethernet port 3 in module 1:

```
Matrix(rw)->set port ingress-filter fe.1.3 enable
```


Downloaded from www.Manualslib.com manuals search engine

show port discard

Use this command to display the frame discard mode for one or more ports.

Syntax

show port discard [*port-string*]

Parameters

port-string	(Optional) Displays the frame discard mode for specific port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.

Defaults

If *port-string* is not specified, frame discarded mode will be displayed for all ports.

Mode

Switch command, Read-Only.

Usage

Ports can be set to discard frames based on whether or not they contain a VLAN tag. They can also be set to discard both frame types or none of the frames received.

Example

This example shows how to display the frame discard mode for Fast Ethernet port 7 in module 2. In this case, the port has been set to discard all tagged frames:

```
Matrix(rw)->show port discard fe.2.7
 Port          Discard Mode
------------  -------------
 fe.2.7          tagged
```

set port discard

Use this command to set the frame discard mode on one or more ports.

Syntax

set port discard *port-string* {**tagged** | **untagged** | **none** | **both**}

Parameters

port-string	Specifies the port(s) for which to set frame discard mode. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.
tagged | **untagged** | **none** | **both**	Sets the port(s) to discard tagged or untagged frames, no frames, or both types of frames.

Defaults

None.

Downloaded from www.Manualslib.com manuals search engine

Mode

Switch command, Read-Write.

Example

This example shows how to set Fast Ethernet port 7 in module2 to discard both tagged and untagged frames:

```
Matrix(rw)->set port discard fe.2.7 both
```

clear port discard

Use this command to reset the frame discard mode to the factory default setting (none).

Syntax

clear port discard *port-string*

Parameters

port-string	Specifies the port(s) for which to reset frame discard mode. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to reset Fast Ethernet port 7 in module module2 to the default discard mode of "none":

```
Matrix(rw)->clear port discard fe.2.7
```


Downloaded from www.Manualslib.com manuals search engine

Configuring the VLAN Egress List

Purpose

To assign or remove ports on the egress list of a particular VLAN. This determines which ports will be eligible to transmit frames for a particular VLAN. For example, ports 1, 5, 9, 8 could be assigned to transmit frames belonging to VLAN 5 (VLAN ID=5).

The port egress type for all ports defaults to tagging transmitted frames, but can be changed to forbidden or untagged. In general, VLANs have no egress (except for VLAN 1) until they are configured by static administration, or through dynamic mechanisms (i.e., GVRP, policy classification or Enterasys dynamic egress).

Setting a port to forbidden prevents it from participating in the specified VLAN and ensures that any dynamic requests (either through GVRP or dynamic egress) for the port to join the VLAN will be ignored. Setting a port to untagged allows it to transmit frames without a tag header. This setting is usually used to configure a port connected to an end user device.

The default VLAN defaults its egress to untagged for all ports.

Commands

For information about...	Refer to page...
show port egress	7-17
set vlan egress	7-18
clear vlan egress	7-19
show vlan dynamic egress	7-20
set vlan dynamicegress	7-20

show port egress

Use this command to display the VLAN membership for one or more ports.

Syntax

show port egress [*port-string*]

Parameters

port-string	(Optional) Displays VLAN membership for specific port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.

Defaults

If *port-string* is not specified, VLAN membership will be displayed for all ports.

Mode

Switch command, Read-Write.

Downloaded from www.Manualslib.com manuals search engine

Example

This example shows you how to show VLAN egress information for Fast Ethernet ports 1 through 3 in module 1. In this case, all three ports are allowed to transmit VLAN 1 frames as tagged and VLAN 10 frames as untagged. Both are static VLANs:

```
Matrix(rw)->show port egress fe.1.1-3
 Port      Vlan           Egress     Registration
Number      Id            Status       Status
-------------------------------------------------------
fe.1.1       1            tagged       static
fe.1.1      10          untagged      static
fe.1.2       1            tagged       static
fe.1.2      10          untagged      static
fe.1.3       1            tagged       static
fe.1.3      10          untagged      static
```

set vlan egress

Use this command to add ports to the VLAN egress list for the device, or to prevent one or more ports from participating in a VLAN. This determines which ports will transmit frames for a particular VLAN.

Syntax

set vlan egress *vlan-list port-string* [**untagged** | **forbidden** | **tagged**]

Parameters

vlan-list	Specifies the VLAN where a port(s) will be added to the egress list.
port-string	Specifies one or more ports to add to the VLAN egress list of the specified *vlan-list*. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.
untagged | **forbidden** | **tagged**	(Optional) Adds the specified ports as: • **untagged** — Causes the port(s) to transmit frames without an IEEE 802.1Q header tag. • **forbidden** — Instructs the device to ignore dynamic requests (either through GVRP or dynamic egress) from the port(s) to join the VLAN and disallows egress on that port. • **tagged** — Causes the port(s) to transmit 802.1Q tagged frames.

Defaults

If **untagged, forbidden** or **tagged** is not specified, the port will be added to the VLAN egress list as tagged.

Mode

Switch command, Read-Write.

Downloaded from www.Manualslib.com manuals search engine

Examples

This example shows how to add Fast Ethernet ports 5 through 10 in module 1 to the egress list of VLAN 7. This means that these ports will transmit VLAN 7 frames as tagged:

```
Matrix(rw)->set vlan egress 7 fe.1.5-10
```

This example shows how to forbid Fast Ethernet ports 13 through 15 in module 1 from joining VLAN 7 and disallow egress on those ports:

```
Matrix(rw)->set vlan egress 7 fe.1.13-15 forbidden
```

This example shows how to allow Fast Ethernet port 2 in module 1 to transmit VLAN 7 frames as untagged:

```
Matrix(rw)->set vlan egress 7 fe.1.2 untagged
```

clear vlan egress

Use this command to remove ports from a VLAN's egress list.

Syntax

clear vlan egress *vlan-list port-string* [**forbidden**]

Parameters

vlan-list	Specifies the number of the VLAN from which a port(s) will be removed from the egress list.
port-string	Specifies one or more ports to be removed from the VLAN egress list of the specified *vlan-list*. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.
forbidden	(Optional) Clears the forbidden setting from the specified port(s) and resets the port(s) as able to egress frames if so configured by either static or dynamic means.

Defaults

If **forbidden** is not specified, tagged and untagged settings will be cleared.

Mode

Switch command, Read-Write.

Examples

This example shows how to remove Fast Ethernet port 14 in module 3 from the egress list of VLAN 9:

```
Matrix(rw)->clear vlan egress 9 fe.3.14
```

This example shows how to remove all Fast Ethernet ports in module 2 from the egress list of VLAN 4:

```
Matrix(rw)->clear vlan egress 4 fe.2.*
```


Downloaded from www.Manualslib.com manuals search engine

show vlan dynamic egress

Use this command to display which VLANs are currently enabled for VLAN dynamic egress.

Syntax

show vlan dynamicegress [*vlan-list*]

Parameters

vlan-list	(Optional) Displays dynamic egress status for specific VLAN(s).

Defaults

If *vlan-list* is not specified, status for all VLANs where dynamic egress is enabled will be displayed.

Mode

Switch command, Read-Only.

Example

This example shows how to display which VLANs are enabled for dynamic egress:

```
Matrix(rw)->show vlan dynamicegress
VLAN 1 is enabled
VLAN 101 is enabled
VLAN 102 is enabled
VLAN 105 is enabled
```

set vlan dynamicegress

Use this command to set the administrative status of one or more VLANs' dynamic egress capability. If VLAN dynamic egress is enabled, the device will add the port receiving a tagged frame to the VLAN egress list of the port according to the frame VLAN ID.

Syntax

set vlan dynamicegress *vlan-list* {**enable** | **disable**}

Parameters

vlan-list	Specifies the number of the VLAN(s) where dynamic egress will be enabled or disabled.
enable | **disable**	Enables or disables dynamic egress.

Defaults

None.

Mode

Switch command, Read-Write.

Downloaded from www.Manualslib.com manuals search engine

Example

This example shows how to enable the dynamic egress function on VLAN 7:

```
Matrix(rw)->set vlan dynamicegress 7 enable
```


Downloaded from www.Manualslib.com manuals search engine

Enabling/Disabling GVRP

Purpose

To dynamically create VLANs across a switched network. The GVRP (GARP VLAN Registration Protocol) command set is used to display GVRP configuration information, the current global GVRP state setting, individual port settings (enable or disable) and timer settings. By default, GVRP is enabled on all ports, and globally on the device.

GARP VLAN Registration Protocol (GVRP) Operation

The following sections describe the device operation when its ports are operating under the Generic Attribute Registration Protocol (GARP) application – GARP VLAN Registration Protocol (GVRP).

Overview

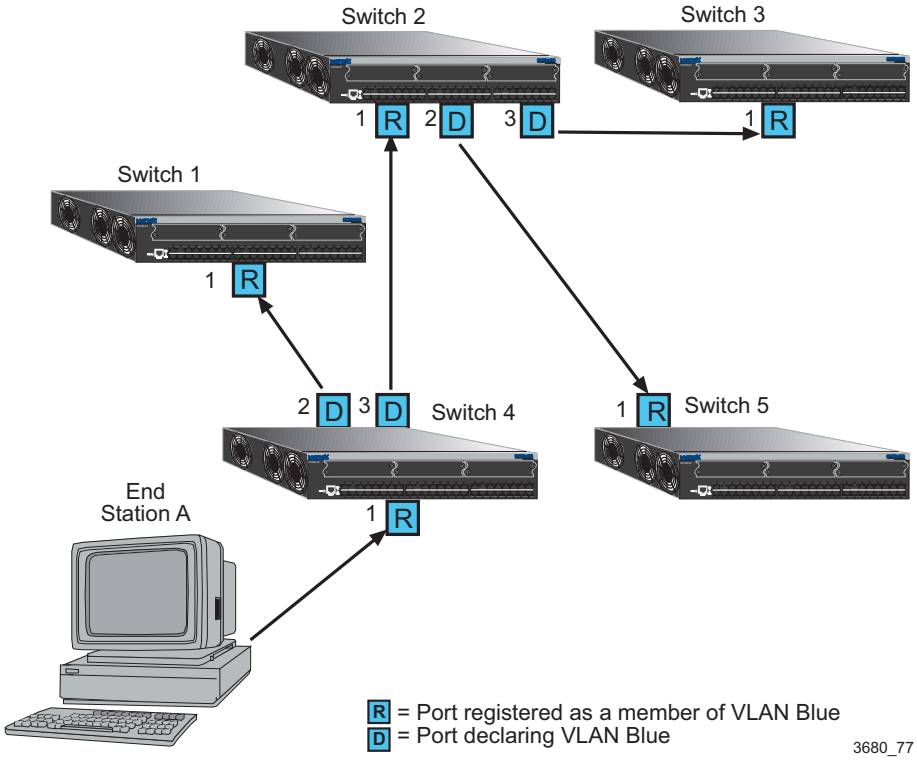
The purpose of GVRP is to dynamically create VLANs across a switched network. When a VLAN is declared, the information is transmitted out GVRP configured ports on the device in a GARP formatted frame using the GVRP multicast MAC address. A switch/router that receives this frame, examines the frame, and extracts the VLAN IDs. GVRP then creates the VLANs and adds the receiving port to its tagged member list for the extracted VLAN ID (s). The information is then transmitted out the other GVRP configured ports of the device. Figure 7-1 shows an example of how VLAN blue from end station A would be propagated across a switch/router network.

How It Works

In Figure 7-1, Device 4, port 1 is registered as being a member of VLAN Blue and then declares this fact out all its ports (2 and 3) to Device 1 and Device 2. These two devices register this in the port egress lists of the ports (Device 1, port 1 and Device 2, port 1) that received the frames with the information. Device 2, which is connected to Device 3 and Device 5 declares the same information to those two devices and the port egress list of each port is updated with the new information, accordingly.

Downloaded from www.Manualslib.com manuals search engine

Figure 7-1 Example of VLAN Propagation via GVRP



Configuring a VLAN on an 802.1Q switch creates a static VLAN entry. The entry will always remain registered and will not time out. However, dynamic entries will time-out and their registrations will be removed from the member list if the end station A is removed. This ensures that, if switches are disconnected or if end stations are removed, the registered information remains accurate.

The end result is that the port egress list of a port is updated with information about VLANs that reside on that port, even if the actual station on the VLAN is several hops away.

Commands

For information about...	Refer to page...
show gvrp	7-24
show garp timer	7-24
set gvrp	7-26
clear gvrp	7-26
set garp timer	7-27
clear garp timer	7-27

Downloaded from www.Manualslib.com manuals search engine

show gvrp

Use this command to display GVRP configuration information.

Syntax

show gvrp [*port-string*]

Parameters

port-string	(Optional) Displays GVRP configuration information for specific port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.

Defaults

If *port-string* is not specified, GVRP configuration information will be displayed for all ports and the device.

Mode

Switch command, Read-Only.

Example

This example shows how to display GVRP status for the device and for Fast Ethernet port 1 in module 2:

```
Matrix(rw)->show gvrp fe.2.1
Global GVRP status is enabled.

Port Number    GVRP status    Last PDU Origin
-----------    -----------    -----------------
fe.2.1         enabled        00-e0-63-97-d4-36
```

Table 7-4 provides an explanation of the command output.

Table 7-4 show gvrp Output Details

Output...	What it displays...
Port Number	Port designation. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.
GVRP status	Whether GVRP is enabled or disabled on the port.
Last PDU Origin	MAC address of the last GVRP frame received on the port.

show garp timer

Use this command to display GARP timer values for one or more ports.

Syntax

show garp timer [*port-string*]

Downloaded from www.Manualslib.com manuals search engine

Parameters

port-string	(Optional) Displays GARP timer information for specific port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.

Defaults

If *port-string* is not specified, GARP timer information will be displayed for all ports.

Mode

Switch command, Read-Only.

Example

This example shows how to display GARP timer information on Fast Ethernet ports 1 through 10 in module 1:



Note: For a functional description of the terms **join**, **leave**, and **leaveall** timers, refer to the standard IEEE 802.1Q documentation, which is not supplied with this device.

```
Matrix(rw)->show garp timer fe.1.1-10
 Port based GARP Configuration: (Timer units are centiseconds)
 Port Number     Join        Leave     Leaveall
 -----------  ----------  ----------  ----------
 fe.1.1             20          60        1000
 fe.1.2             20          60        1000
 fe.1.3             20          60        1000
 fe.1.4             20          60        1000
 fe.1.5             20          60        1000
 fe.1.6             20          60        1000
 fe.1.7             20          60        1000
 fe.1.8             20          60        1000
 fe.1.9             20          60        1000
 fe.1.10            20          60        1000
```

Table 7-5 provides an explanation of the command output. For details on using the **set gvrp** command to enable or disable GVRP, refer to "set gvrp" on page 7-26. For details on using the **set garp timer** command to change default timer values, refer to "set garp timer" on page 7-27.

Table 7-5 show gvrp configuration Output Details

Output...	What it displays...
Port Number	Port designation. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.
Join	Join timer setting.
Leave	Leave timer setting.
Leaveall	Leavall timer setting.

Downloaded from www.Manualslib.com manuals search engine

set gvrp

Use this command to enable or disable GVRP globally on the device or on one or more ports.

Syntax

set gvrp {**enable** | **disable**} [*port-string*]

Parameters

disable | **enable**	Disables or enables GVRP on the device.
port-string	(Optional) Disables or enables GVRP on specific port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.

Defaults

If *port-string* is not specified, GVRP will be disabled or enabled for all ports.

Mode

Switch command, Read-Write.

Examples

This example shows how to enable GVRP globally on the device:

```
Matrix(rw)->set gvrp enable
```

This example shows how to disable GVRP globally on the device:

```
Matrix(rw)->set gvrp disable
```

This example shows how to enable GVRP on Fast Ethernet port 3 in module 1:

```
Matrix(rw)->set gvrp enable fe.1.3
```

clear gvrp

Use this command to clear GVRP status or on one or more ports.

Syntax

clear gvrp [*port-string*]

Parameters

port-string	(Optional) Clears GVRP status on specific port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.

Defaults

If *port-string* is not specified, GVRP status will be cleared for all ports.

Mode

Switch command, Read-Write.

Downloaded from www.Manualslib.com manuals search engine

Example

This example shows how to clear GVRP status globally on the device:

```
Matrix(rw)->clear gvrp
```

set garp timer

Use this command to adjust the values of the join, leave, and leaveall timers.

Syntax

set garp timer {[**join** *timer-value*] [**leave** *timer-value*] [**leaveall** *timer-value*]} *port-string*

Parameters

join *timer-value*	Sets the GARP join timer in centiseconds (Refer to 802.1Q standard.)
leave *timer-value*	Sets the GARP leave timer in centiseconds (Refer to 802.1Q standard.)
leaveall *timer-value*	Sets the GARP leaveall timer in centiseconds (Refer to 802.1Q standard.)
port-string	Specifies the port(s) on which to configure GARP timer settings. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.

Defaults

None.

Mode

Switch command, Read-Write.

Usage

The setting of these timers is critical and should only be changed by personnel familiar with the 802.1Q standards documentation, which is not supplied with this device.

Examples

This example shows how to set the GARP join timer value to 100 centiseconds for all ports:

```
Matrix(rw)->set garp timer join 100 *.*.*
```

This example shows how to set the leave timer value to 300 centiseconds for all ports:

```
Matrix(rw)->set garp timer leave 300 *.*.*
```

This example shows how to set the leaveall timer value to 20000 centiseconds for all ports:

```
Matrix(rw)->set garp timer leaveall 20000 *.*.*
```

clear garp timer

Use this command to reset GARP timers back to default values.

Syntax

clear garp timer {[**join**] [**leave**] [**leaveall**]} *port-string*

Downloaded from www.Manualslib.com manuals search engine

Parameters

join	(Optional) Resets the join timer to 20 centiseconds.
leave	(Optional) Resets the leave timer to 60 centiseconds.
leaveall	(Optional) Resets the leaveall timer to 1000 centiseconds.
port-string	Specifies the port(s) on which to reset GARP timer(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.

Defaults

At least one optional parameter must be entered.

Mode

Switch command, Read-Write.

Example

This example shows how to reset the GARP leave timer to 60 centiseconds on Fast Ethernet port 5 in module 2:

```
Matrix(rw)->clear garp timer leave fe.2.5
```


Downloaded from www.Manualslib.com manuals search engine

8

Policy Classification Configuration

This chapter describes the Policy Classification set of commands and how to use them.

Note: It is recommended that you use Enterasys NetSight Policy Manager as an alternative to CLI for configuring policy classification on the Enterasys Matrix Series devices.

For information about...	Refer to page...
Policy Classification Configuration Summary	8-1
Configuring Policy Profiles	8-2
Assigning Classification Rules to Policy Profiles	8-7
Configuring Policy Class of Service (CoS)	8-21
Configuring Policy-Based Routing	8-42
Configuring Policy-Based Routing	8-42

Policy Classification Configuration Summary

Enterasys Matrix Series devices support policy profile-based provisioning of network resources by allowing IT administrators to:

- Create, change or remove user profiles based on business-specific use of network services.
- Permit or deny access to specific services by creating and assigning classification rules which map user profiles to protocol-based frame filtering policies configured for a particular VLAN or Class of Service (CoS).
- Assign or unassign ports to policy profiles so that only ports activated for a profile will be allowed to transmit frames accordingly.
- Configure CoS to automatically assign policy-based inbound rate limiters and transmit queues.

Note: Enterasys Matrix Series devices also support policy-based routing, which forwards or drops packets at Layer 3 according to matching access lists (ACLs) in route maps configured on routing interfaces. For details, refer to “Configuring Denial of Service (DoS) Prevention” on page 24-22.

Downloaded from www.Manualslib.com manuals search engine

Configuring Policy Profiles

Purpose

To review, create, change and remove policy profiles for managing network resources.

Commands

For information about...	Refer to page...
show policy profile	8-2
set policy profile	8-3
clear policy profile	8-5
show policy invalid	8-5
set policy invalid action	8-6
clear policy invalid action	8-6
Assigning Classification Rules to Policy Profiles	8-7

show policy profile

Use this command to display policy profile information.

Syntax

show policy profile {**all** | *profile-index* [*consecutive-pids*] [**-verbose**]}

Parameters

all | *profile-index*	Displays policy information for all profile indexes or a specific profile index.
consecutive-pids	(Optional) Displays information for specified consecutive profile indexes.
-verbose	(Optional) Displays detailed information.

Defaults

If optional parameters are not specified, summary information will be displayed for the specified index or all indexes.

Mode

Switch command, Read-Only.

Example

This example shows how to display policy information for policy profile 11:

```
Matrix(rw)->show policy profile 11
Profile Index           :11
Profile Name            :MacAuth1
```


Downloaded from www.Manualslib.com manuals search engine

```
Row Status              :active
Port VID Status         :enabled
Port VID Override       :11
CoS Status              :disabled
CoS                     :0
Tagged Egress VLAN List :11
Forbidden VLAN List     :none
Untagged VLAN List      :none
Replace TCI Status      :enabled
Admin Profile Usage     :none
Oper Profile Usage      :fe.2.1-2
Dynamic Profile Usage   :fe.2.1-2
```

Table 8-1 provides an explanation of the command output.

Table 8-1 show policy profile Output Details

Output...	What it displays...
Profile Index	Number of the policy profile.
Profile Name	User-supplied name assigned to this policy profile.
Row Status	Whether or not the policy profile is enabled (**active**) or disabled.
Port VID Status	Whether or not PVID override is **enabled** or **disabled** for this policy profile. If all the classification rules associated with this profile are missed, then this parameter, if specified, determines default behavior.
Port VID Override	The PVID to assign to packets, if PVID override is enabled.
CoS Status	Whether or not Class of Service override is **enabled** or **disabled** for this profile. If all the classification rules associated with this profile are missed, then this parameter, if specified, determines default behavior.
CoS	The CoS priority value to assign to packets, if CoS override is enabled.
Tagged Egress VLAN List	VLAN(s) that ports to which the policy profile is assigned can use for tagged egress.
Forbidden VLAN List	VLAN(s) forbidden to ports to which the policy profile is assigned.
Untagged VLAN List	VLAN(s) that ports to which the policy profile is assigned can use for untagged egress.
Admin Profile Usage	Ports administratively assigned to use this policy profile.
Oper Profile Usage	Ports currently assigned to use this policy profile.
Dynamic Profile Usage	Port dynamically assigned to use this policy profile.

set policy profile

Use this command to create a policy profile entry.

Syntax

set policy profile *profile-index* [**name** *name*] [**pvid-status** {**enable** | **disable**}] [**pvid** *pvid*] [**cos-status** {**enable** | **disable**}] [**cos** *cos*] [**egress-vlans** *egress-vlans*] [**forbidden-vlans** *forbidden-vlans*] [**untagged-vlans** *untagged-vlans*] [**append**] [**clear**]

Downloaded from www.Manualslib.com manuals search engine

Parameters

profile-index	Specifies an index number for the policy profile. Valid values are **1** - **1023**.
name *name*	(Optional) Specifies a name for the policy profile. This is a string from 1 to 64 characters.
pvid-status enable | **disable**	(Optional) Enables or disables PVID override for this policy profile. If all the classification rules associated with this profile are missed, then this parameter, if specified, determines default behavior.
pvid *pvid*	(Optional) Specifies the PVID to assign to packets, if PVID override is enabled and invoked as the default behavior.
cos-status enable | **disable**	(Optional) Enables or disables Class of Service override for this policy profile. If all the classification rules associated with this profile are missed, then this parameter, if specified, determines default behavior.
cos *cos*	(Optional) Specifies a COS value to assign to packets, if CoS override is enabled and invoked as the default behavior. Valid values are 0 to 255.
egress-vlans *egress-vlans*	(Optional) Specifies that the port to which this policy profile is applied should be added to the egress list of the VLANs defined by *egress-vlans*. Packets will be formatted as tagged.
forbidden-vlans *forbidden-vlans*	(Optional) Specifies that the port to which this policy profile is applied should be added as forbidden to the egress list of the VLANs defined by *forbidden-vlans*. Packets from this port will not be allowed to participate in the listed VLANs.
untagged-vlans *untagged-vlans*	(Optional) Specifies that the port to which this policy profile is applied should be added to the egress list of the VLANs defined by *untagged-vlans*. Packets will be formatted as untagged.
append	(Optional) Appends this policy profile setting to settings previously specified for this policy profile by the **egress-vlans**, **forbidden-vlans**, or **untagged-vlans** parameters. If **append** is not used, previous VLAN settings are replaced.
clear	(Optional) Clears this policy profile setting from settings previously specified for this policy profile by the **egress-vlans**, **forbidden-vlans**, or **untagged-vlans** parameters.

Defaults

If optional parameters are not specified, none will be applied.

Mode

Switch command, Read-Write.

Example

This example shows how to create a policy profile 1 named “netadmin” with PVID override enabled for PVID 10, and Class-of-Service override enabled for CoS 5. This profile can use VLAN 10 for untagged egress:

```
Matrix(rw)->set policy profile 1 name netadmin pvid-status enable pvid 10 cos-
status enable cos 5 untagged-vlans 10
```


Downloaded from www.Manualslib.com manuals search engine

clear policy profile

Use this command to delete a policy profile entry.

Syntax

clear policy profile *profile-index*

Parameters

profile-index	Specifies the index number of the policy profile entry to be deleted. Valid values are **1** to **1023**.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to delete policy profile 8:

```
Matrix(rw)->clear policy profile 8
```

show policy invalid

Displays information about the action the device will apply on an invalid or unknown policy.

Syntax

show policy invalid {**action** | **count** | **all**}

Parameters

action | **count** | **all**	Shows the action the device should take if asked to apply an invalid or unknown policy, or the number of times the device has detected an invalid/unknown policy, or both action and count information.

Defaults

None.

Mode

Switch command, Read-Only.

Example

This example shows how to display invalid policy action and count information:

```
Matrix(rw)->show policy invalid all
Current action on invalid/unknown profile is: Forward packets
Number of invalid/unknown profiles detected: 4
```


Downloaded from www.Manualslib.com manuals search engine

set policy invalid action

Use this command to assign the action the device will apply to an invalid or unknown policy.

Syntax

set policy invalid action {**default-policy** | **drop** | **forward**}

Parameters

default-policy	Instructs the device to ignore this result and search for the next policy assignment rule.
drop	Instructs the device to block traffic.
forward	Instructs the device to forward traffic as if no policy has been assigned.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to assign a drop action to invalid policies:

```
Matrix(rw)->set policy invalid action drop
```

clear policy invalid action

Use this command to reset the action the device will apply to an invalid or unknown policy to the default action of applying the default policy.

Syntax

clear policy invalid action

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to reset the invalid policy action:

```
Matrix(rw)->clear policy invalid action
```


Downloaded from www.Manualslib.com manuals search engine

Assigning Classification Rules to Policy Profiles

Purpose

To review, assign and unassign classification and admin rules. Classification rules map policy profiles to protocol-based frame filtering policies configured for a particular VLAN or Class of Service (CoS). Admin rules assign policy profiles to incoming traffic.

Commands

For information about...	Refer to page...
show policy rule	8-7
show policy capability	8-10
set policy classify	8-11
set policy rule	8-13
clear policy rule	8-15
clear policy all-rules	8-16
set policy port	8-17
show policy allowed-type	8-17
set policy allowed-type	8-18
clear policy allowed-type	8-19
clear policy port-hit	8-19

show policy rule

Use this command to display policy classification and admin rule information.

Syntax

show policy rule [**attribute**] | [**all**] | [**admin-profile**] | [*profile-index*] [**ether** | **ipdest** | **ipfrag** | **ipproto** | **ipsource** | **iptos** | **llcDsapSsap** | **macdest** | **macsource** | **port** | **tcpdestport**| **tcpsourceport**| **udpdestport** | **udpsourceport** [*data*] [**mask** *mask*] [**port-string** *port-string*] [**rule-status** {**active** | **not-in-service** | **not-ready**}] [**storage-type** {**non-volatile** | **volatile**}] [**vlan** *vlan*] | [**drop** | **forward**] [**dynamic-pid** *dynamic-pid*] [**cos** *cos*] [**admin-pid** *admin-pid*] [**-verbose**]

Parameters

attribute	Displays the attributes of the specified rules.
all | **admin-profile** | *profile-index*	Displays **all** admin and classification rules, rules for the admin profile, or for a specific *profile-index* number. Valid index values are **1** - **1023**.
ether	Displays Ethernet type II rules.
ipdest	Displays IP destination address rules.
ipfrag	Displays IP fragmentation rules.
ipproto	Displays IP protocol field in IP packet rules.

Downloaded from www.Manualslib.com manuals search engine

ipsource	Displays IP source address rules.
iptos	Displays Type of Service rules.
llcDsapSsap	Displays 802.3 DSAP/SSAP rules.
macdest	Displays MAC destination address rules.
macsource	Displays MAC source address rules.
port	Displays port related rules.
tcpdestport	Displays TCP destination port rules.
tcpsourceport	Displays TCP source port rules.
udpdestport	Displays UDP destination port rules.
udpsourceport	Displays UDP source port rules.
data	(Not required for **ipfrag** classification.) Displays rules for a predefined classifier. This value is dependent on the classification type entered. Refer to Table 8-3 for valid values for each classification type.
mask *mask*	(Optional) Displays rules for a specific data mask. Refer to Table 8-3 for valid values for each classification type and data value.
port-string *port-string*	(Optional) Displays rules related to a specific ingress port.
rule-status active | **not-in-service** | **not-ready**	(Optional) Displays rules related to a specific rules status.
storage-type non-volatile | **volatile**	(Optional) Displays rules configured for either non-volatile or volatile storage.
vlan vlan	(Optional) Displays rules for a specific VLAN ID.
drop | **forward**	Displays rules based on whether matching packets specified by the **vlan** parameter will be dropped or forwarded.
dynamic-pid *dynamic-pid*	Displays rules associated with a specific dynamic policy profile index ID.
cos *cos*	(Optional) Displays rules for a Class-of-Service value.
admin-pid admin-pid	Displays rules associated with a specific administrative policy profile index ID.
-verbose	(Optional) Displays detailed information.

Defaults

- If *port-string*, rule status, storage type, Syslog state, trap, and usage-list are not specified, all rules related to other specifications will be displayed.
- If **verbose** is not specified, summary information will be displayed.

Mode

Switch command, Read-Only.

Examples

This example shows how to display policy classification information for Ethernet type 2 rules

```
Matrix(rw)->show policy rule ether:
```


Downloaded from www.Manualslib.com manuals search engine

```
|PID  |Rule Type    |Rule Data           |Mk|PortStr   |RS|ST|S|T|D|VLAN|CoS |U|
| 1   |Ether        |32923 (0x809B)      |16|All       | A|NV|Y|Y| | 105|    |?|
| 1   |Ether        |33011 (0x80F3)      |16|All       | A|NV|Y|Y| | 105|    |?|
| 1   |Ether        |33079 (0x8137)      |16|All       | A|NV|Y|Y| | 101|    |?|
| 1   |Ether        |33080 (0x8138)      |16|All       | A|NV|Y|Y| | 101|    |?|
| 1   |Ether        |33276 (0x81FC)      |16|All       | A|NV|Y|Y| |drop|    |?|
| 2   |Ether        |32923 (0x809B)      |16|All       | A|NV|Y|Y| | 105|    |?|
| 2   |Ether        |33011 (0x80F3)      |16|All       | A|NV|Y|Y| | 105|    |?|
| 2   |Ether        |33079 (0x8137)      |16|All       | A|NV|Y|Y| | 101|    |?|
```

This example shows how to display admin rule information for the policy profile with index number 1 :

```
Matrix(rw)->show policy rule admin-pid 1

|Admin|Rule Type   |Rule Data           |Mk|PortStr   |RS|ST|S|T|D|dPID|aPID|U|
|admin|Port        |fe.1.1              |16|fe.1.1    | A|NV| | | |    |   1|?|
|admin|Port        |fe.1.2              |16|fe.1.2    | A|NV| | | |    |   1|?|
|admin|Port        |fe.1.3              |16|fe.1.3    | A|NV| | | |    |   1|?|
|admin|Port        |fe.1.4              |16|fe.1.4    | A|NV| | | |    |   1|?|
|admin|Port        |fe.1.5              |16|fe.1.5    | A|NV| | | |    |   1|?|
|admin|Port        |fe.1.6              |16|fe.1.6    | A|NV| | | |    |   1|?|
```

Table 8-2 provides an explanation of the command output.

Table 8-2 show policy rule Output Details

Output...	What it displays...
PID	Profile profile index number, indicating a classification rule is displayed. Assigned to this classification rule with the **set policy profile** command (“set policy profile” on page 8-3).
Admin	Indicates an admin rule is displayed.
Rule Type	Whether the rule protocol-based or port-based. Refer to Table 8-3 for valid classification types.
Rule Data	Rule data value. Refer to Table 8-3 for valid values for each classification type.
Mk	Rule data mask. Refer to Table 8-3 for valid values for each classification data value.
PortStr	Ingress port(s) to which this rule applies.
RS	Whether or not the status of this rule is active (A), not in service or not ready.
ST	Whether or not this rule’s storage type is non-volatile (NV) or volatile (V).
Vlan	VLAN ID to which this rule applies and whether or not matching packets will be dropped or forwarded.
CoS	Class of Service value to which this rule applies.
dPID	Whether or not this is a dynamic profile ID.
aPID	Whether or not this is an administrative profile index ID.

Downloaded from www.Manualslib.com manuals search engine

show policy capability

Use this command to display all policy classification capabilities supported by your Enterasys Matrix Series device.

Syntax

show policy capability

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Only.

Usage

The output of this command shows a table listing classifiable traffic attributes and the type of actions, by rule type, that can be executed relative to each attribute. Above the table is a list of all the actions possible on this device.

The left-most column of the table lists all possible classifiable traffic attributes. The next two columns from the left indicate how policy profiles may be assigned, either administratively or dynamically. The next four columns from the left indicate the actions that may be performed. The last three columns indicate auditing options.

An x in an action column for a traffic attribute row indicates that your system has the capability to perform that action for traffic classified by that attribute.

Example

This example shows how to display your Enterasys Matrix Series device's policy classification capabilities. In this case, Enterasys Matrix DFE-Platinum Series capabilities are shown. Refer to "set policy rule" on page 8-13 for a description of the parameters displayed:

```
Matrix(rw)->show policy capability
The following supports related to policy are supported in this device:
VLAN Forwarding         Priority                Permit
Deny                    TCI Overwrite           Rule-Use Notification
Rules Table             Rule-Use Accounting
Longest Prefix Rules    Port Disable Action
 ============================================================
|                          | D |   |   |   | F |   |   | D |
|                          | Y |   |   |   | O | S |   | I |
|                          | N | A |   |   | R | Y |   | S |
|                          | A | D | V |   | D | W | S | T | A |
|                          | M | M | L | C | R | A | L | R | B |
|                          | I | I | A | O | O | R | O | A | L |
| SUPPORTED RULE TYPES     | C | N | N | S | P | D | G | P | E |
 ============================================================
```


Downloaded from www.Manualslib.com manuals search engine

MAC source address	X	X	X	X	X	X	X	X	X
MAC destination address	X	X	X	X	X	X	X	X	X
IPX source address	X	X	X	X	X	X	X	X	X
IPX destination address	X	X	X	X	X	X	X	X	X
IPX source socket	X	X	X	X	X	X	X	X	X
IPX destination socket	X	X	X	X	X	X	X	X	X
IPX transmission control	X	X	X	X	X	X	X	X	X
IPX type field	X	X	X	X	X	X	X	X	X
IPv6 source address									
IPv6 destination address									
IPv6 flow label									
IP source address	X	X	X	X	X	X	X	X	X
IP destination address	X	X	X	X	X	X	X	X	X
IP fragmentation	X	X	X	X	X	X	X	X	X
UDP port source	X	X	X	X	X	X	X	X	X
UDP port destination	X	X	X	X	X	X	X	X	X
TCP port source	X	X	X	X	X	X	X	X	X
TCP port destination	X	X	X	X	X	X	X	X	X
ICMP packet type	X	X	X	X	X	X	X	X	X
TTL									
IP type of service	X	X	X	X	X	X	X	X	X
IP proto	X	X	X	X	X	X	X	X	X
Ether II packet type	X	X	X	X	X	X	X	X	X
LLC DSAP/SSAP/CTRL	X	X	X	X	X	X	X	X	X
VLAN tag	X	X	X	X	X	X	X	X	X
Replace tci	X	X	X	X	X	X	X	X	X
Port string	X	X	X	X	X	X	X	X	X

set policy classify

Use this command to assign incoming untagged frames to a specific policy profile, classification and to VLAN or Class-of-Service classification rules.

Syntax

set policy classify *profile-index classify-index* {**vlan** | **cos**} {*classify-value* | **forward** | **drop**} {**ether** | **llc** | **iptos** | **ipproto** | **ipxclass** | **ipxtype** | **ipsource** | **ipdest** | **ipxsource** | **ipxdest** | **udpportsource** | **udpportdest** | **tcpportsource** | **tcpportdest** | **ipxsourcesocket** | **ipxdestsocket** | **macsource** | **macdest** | **ipfrag** | **icmptype** | **vlantag** | **tci** | **port**} [*class-data-val*] [*class-data-mask*]

Downloaded from www.Manualslib.com manuals search engine

Parameters

profile-index	Specifies that this is an administrative rule or associates this classification rule with a policy profile index configured with the **set policy profile** command ("set policy profile" on page 8-3). Valid *profile-index* values are **1**- **63**.
classify-index	Policy Classification Index (1-65535)
vlan	Specifies Vlan Classification Rule
cos	Specifies Class Of Service Classification Rule
classify-value	vlan / Class Of Service (0-4095)
forward	Specifies Forwarding of packet
drop	Specifies Dropping of packet
ether	Classifies based on type field in Ethernet II packet.
llc	DSAP/SSAP pair in 802.3 type packet field - (0 - 65535)
iptos	Classifies based on Type of Service field in IP packet.
ipproto	Classifies based on protocol field in IP packet.
ipsource	Classifies based on source IP address
ipdest	Classifies based on destination IP address
udpportsource	Classifies based on UDP port source - supported class-data-val: 0 - 65535
udpportdest	Classifies based on UDP port destination - supported class-data-val: 0 - 65535
tcpportsource	Classifies based on TCP port source - supported class-data-val: 0 - 65535
tcpportdest	Classifies based on TCP port destination - supported class-data-val: 0 - 65535
macsource	Classifies based on MAC source address.
macdest	Classifies based on MAC destination address.
ipfrag	Classifies based on IP fragmentation value.
port	Classifies based on port-string.
class-data-val	Data Value of meaning
class-data-mask	Number of mask bits to apply to Data Value

Defaults

If *mask* is not specified, all data bits will be considered relevant.

Mode

Switch command, Read-Write.

Usage

Classification rules are automatically enabled when created.

Downloaded from www.Manualslib.com manuals search engine

Examples

This example shows how to use Table 8-3 to create (and enable) a VLAN classification rule to policy 2, classification 65, to drop packets from a source IP address of 172.16.1.2:

```
Matrix(rw)->set policy classify 2 65 vlan drop ipsource 172.16.1.2
```

set policy rule

Use this command to assign incoming untagged frames to a specific policy profile and to VLAN or Class-of-Service classification rules.

Syntax

set policy rule admin-profile | *profile-index* {**ether** |**ipfrag** | **ipproto** | **ipdest** | **ipsource** | **iptos** | **llcDsapSsap** | **macdest** | **macsource** | | **port** | **tcpdestport** | **tcpsourceport** | **udpdestport** | **udpsourceport**} *data* [**mask** *mask*] [**port-string** *port-string*] [**storage-type** {**non-volatile** | **volatile**}] [**vlan** *vlan*] | [**drop** | **forward**] [**admin-pid** *admin-pid*] [**cos** *cos*]

Parameters

admin-profile | *profile-index*	Specifies that this is an administrative rule or associates this classification rule with a policy profile index configured with the **set policy profile** command ("set policy profile" on page 8-3). Valid *profile-index* values are **1**- **1023**. **Note:** Admin profiles can be assigned to a specific ingress port by specifying **port-string** and **admin-pid** values as described below.
ether	Classifies based on type field in Ethernet II packet.
ipdest	Classifies based on destination IP address.
ipfrag	Classifies based on IP fragmentation value.
ipproto	Classifies based on protocol field in IP packet.
ipsource	Classifies based on source IP address.
iptos	Classifies based on Type of Service field in IP packet.
llcDsapSsap	Classifies based on DSAP/SSAP pair in 802.3 type packet.
macdest	Classifies based on MAC destination address.
macsource	Classifies based on MAC source address.
port	Classifies based on port-string.
tcpdestport	Classifies based on TCP destination port with.
tcpsourceport	Classifies based on TCP source port .
udpdestport	Classifies based on UDP destination port .
udpsourceport	Classifies based on UDP source port .
data	(Not required for **ipfrag** classification.) Specifies the code for a predefined classifier. This value is dependent on the classification type entered. Refer to Table 8-3 for valid values for each classification type.
mask *mask*	(Optional) Specifies the number of significant bits to match, dependent on the *data* value entered. Refer to Table 8-3 for valid values for each classification type and data value.

Downloaded from www.Manualslib.com manuals search engine

port-string *port-string*	(Optional) If **admin-profile** is specified, applies this administratively-assigned rule to a specific ingress port. **Note:** Enterasys Matrix Series devices with firmware versions 3.00.xx and higher also support this alternative command to administratively assign a profile rule to a port: **set policy port** *port-string admin-id*
storage-type non-volatile | volatile	Adds or removes this entry from non-volatile storage.
vlan vlan	Classifies to a VLAN ID.
drop | forward	Specifies that packets within this classification will be dropped or forwarded.
admin-pid admin-pid	If **admin-profile** is specified, associates this rule with a policy profile index ID. Valid values are **1** - **1023**.
cos *cos*	Specifies that this rule will classify to a Class-of-Service ID. Valid values are **0** - **255**, and can be configured using the **set cos settings** command as described in "set cos settings" on page 8-39. A value of -1 indicates that no CoS forwarding behavior modification is desired.

Defaults

- If *mask* is not specified, all data bits will be considered relevant.
- If *port-string* is not specified, rule will be scoped to all ports.

Mode

Switch command, Read-Write.

Usage

Classification rules are automatically enabled when created.

Examples

This example shows how to use Table 8-3 to create (and enable) a classification rule to associate with policy number 1. This rule will filter Ethernet II Type 1526 frames to VLAN 7:

```
Matrix(rw)->set policy rule 1 ether 1526 vlan 7
```

This example shows how to use Table 8-3 to create (and enable) a classification rule to associate with policy profile number 5. This rule specifies that UDP frames from source port 45 will be filtered to VLAN 7:

```
Matrix(rw)->set policy rule 5 udpportsourceip 45 vlan 7
```

This example shows how to configure classification rule 2 as an administrative profile and assign it to ingress port fe.1.1:

```
Matrix(rw)->set policy rule admin-profile port fe.1.1 port-string fe.1.1 admin-pid 2
Matrix(rw)->set policy rule admin-profile ether 1526 admin-pid 2
```

Table 8-3 provides the **set policy rule** *data* values that can be entered for a particular classification type, and the *mask* bits that can be entered for each classifier associated with that parameter.

Downloaded from www.Manualslib.com manuals search engine

Table 8-3 Valid Values for Policy Classification Rules

Classification Rule Parameter	*data* value	*mask* bits
ether	Type field in Ethernet II packet: **1536** - **65535**	**1**- **16**
Destination or Source IP Address: **ipdest** **ipsource**	IP Address in dotted decimal format: **000.000.000.000**	**1** - **48**
ipfrag	Not applicable.	Not applicable.
ipproto	Protocol field in IP packet: **0** - **255**	**1**- **8**
iptos	Type of Service field in IP packet: **0** - **255**	**1**- **8**
llcDsapSsap	DSAP/SSAP/CTRL field in llc: **a-b-c-ab**	**1** - **40**
Destination or Source MAC: **macdest** **macsource**	MAC Address: **00-00-00-00-00-00**	**1** - **48**
port	Port string: Eg. **fe.1.1**	**1** - **16**
Destination or Source TCP port: **tcpdestport** **tcpsourceport**	TCP Port Number : **ab 0-65535:1.1.1.1;** or **0-0xFFFF:1.1.1.1**	**1** - **48**
Destination or Source UDP port: **udpsourceport** **udpdestport**	UDP Port Number : **ab 0-65535:1.1.1.1;** or **0-0xFFFF:1.1.1.1**	**1** - **48**

clear policy rule

Use this command to delete one or all policy classification rule entries.

Syntax

clear policy rule admin-profile | *profile-index* **all-pid-entries** | **ether ipdest** | **ipfrag** | **ipproto** | **ipsource**| **iptos** |**llcDsapSsap** | **macdest** | **macsource** | **port** |**tcpdestport**| **tcpsourceport**| **udpdestport**| **udpsourceport**] [**all-traffic-entries** | *data*][**mask** *mask*] [**port-string** *port-string*]}

Parameters

admin-profile | *profile-index*	Deletes an administrative profile rule, or deletes rule(s) associated with a specific profile number. Valid *profile-index* values are **1** - **1023**.
all-pid-entries	Deletes all rules associated with the specified policy profile index ID.
ether	Deletes associated Ethernet II classification rule.
ipdest	Deletes associated IP destination classification rule.
ipfrag	Deletes associated IP fragmentation classification rule.
ipproto	Deletes associated IP protocol classification rule.
ipsource	Deletes associated IP source classification rule.
iptos	Deletes associated IP Type of Service classification rule.
llcDsapSsap	Deletes associated DSAP/SSAP classification rule.

Downloaded from www.Manualslib.com manuals search engine

macdest	Deletes associated MAC destination address classification rule.
macsource	Deletes associated MAC source address classification rule.
port	Deletes associated port-string classification rule.
tcpdestport	Deletes associated TCP destination port classification rule .
tcpsourceport	Deletes associated TCP source port classification rule .
udpdestport	Deletes associated UDP destination port classification rule .
udpsourceport	Deletes associated UDP source port classification rule .
all-traffic-entries | *data*	(Optional) Deletes all entries associated with this traffic rule or a specific data value entry. Refer to Table 8-3 for valid values for each classification type.
mask *mask*	(Optional) Deletes associated data mask. Refer to Table 8-3 for valid values for each classification type and data value.
port-string *port-string*	(Optional) Deletes specified rule entries for specific ingress port(s).

Defaults

When applicable, *data*, *mask*, and *port-string* must be specified for individual rules to be cleared.

Mode

Switch command, Read-Write.

Example

This example shows how to delete all classification rule entries associated with policy profile 1 from all ports:

```
Matrix(rw)->clear policy rule 1 all-pid-entries
```

clear policy all-rules

Use this command to remove all admin and classification rules.

Syntax

clear policy all-rules

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to remove all administrative and classification rules:

```
Matrix(rw)->clear policy all-rules
```


Downloaded from www.Manualslib.com manuals search engine

set policy port

Use this command to assign an administrative rule to a port.

Syntax

set policy port *port-name admin-id*

Parameters

port-name	Specifies the port(s) on which to set assign an administrative rule. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.
admin-id	Specify a policy profile index number with a valid range of [1..63].

Defaults

None.

Mode

Switch command, Read-Write.

Usage

The **set policy rule** command ("set policy rule" on page 8-13) used with the **admin-profile** parameter will associate a classification rule with a policy profile index number, thus making an administrative rule.

Example

This example shows how to assign an administrative rule with an index of 20 to port fe.1.3:

```
Matrix(rw)->set policy port fe.1.3 20
```

show policy allowed-type

Use this command to display a list of currently supported traffic rules applied to the admininstrative profile for one or more ports.

Syntax

show policy allowed-type *port-string* [**-verbose**]

Parameters

port-string	Specifies port(s) for which to display traffic rules.
-verbose	(Optional) Displays detailed information.

Defaults

If **-verbose** is not specified, summary information will be displayed.

Mode

Switch command, Read-Only.

Downloaded from www.Manualslib.com manuals search engine

Example

This example shows how to show information about policies allowed on port ge.1.5:

```
Matrix(rw)->show policy allowed-type ge.1.5
SUPPORTED AND ALLOWED TRAFFIC RULE TYPES

 o Means Traffic Rule Type is supported on this bridge port
 * Means Traffic Rule Type is supported and allowed on this bridge port

=========================================================================
|              |   TRAFFIC  RULE  TYPES                                  |
+--------------+---+-----------+-----+-----+---+---+-+-----+---+---+-+-+
|              |   |           |     |     |   |   | |     |   |   | | |
|              |MAC|   IPX     |IPv6 | IP  |UDP|TCP| | IP  |   |   | | |
|              |   |           |     |     |   |   | |     |   |   | | |
|              |   |    S D    |     |     |   |   | |     |E  |   | | |
|              |   |    S S   T|    F|    F|   |   |I|    T|N  |V  |P|
|              |S D|S D O O C Y|S D L|S D R|S D|S D|C|T T Y|E L|L T|O|
|              |R S|R S C C O P|R S O|C S A|R S|R S|M|T O P|T L|A C|R|
|              |C T|C T K K S E|C T W|R T G|C T|C T|P|L S E|2 C|N I|T|
|              |---+-----------+-----+-----+---+---+-+-----+---+---+-+-+
|              |   |           |  1 1|1 1 1|1 1|1 1|1|2 2 2|2 2|2 2|3|
|     Port     |1 2|3 4 5 6 7 8|9 0 1|2 3 4|5 6|7 8|9|0 1 2|5 6|7 8|1|
=========================================================================
| ge.1.5 |* *|* * * * * *|     |* * *|* *|* *|*|  * *|* *|* *|* *|*|
```

set policy allowed-type

Use this command to assign a list of traffic rules that can be applied to the admin profile for one or more ports.

Syntax

set policy allowed-type *port-string* **traffic-rule** *rule-list* [**append** | **clear**]

Parameters

port-string	Specifies port(s) on which to apply traffic rules.
traffic-rule *rule-list*	Specifies traffic rules to be allowed. This is a numeric value displayed in the **show policy allowed-type** output ("show policy allowed-type" on page 8-17). Entering "none" means that no traffic rules will be allowed on this port.
append | **clear**	(Optional) Appends traffic rule(s) to the port(s) current rules, or clears specified rules.

Defaults

If **append** or **clear** is not specified, rule(s) will be appended to the port's current list.

Downloaded from www.Manualslib.com manuals search engine

Mode

Switch command, Read-Write.

Examples

This example shows how to allow only rule type 1 (source MAC address classification) to be applied to the admin profile for port ge.1.5:

```
Matrix(rw)->set policy allowed-type ge.1.5 traffic-rule 1
```

This example shows how to clear only rule type 27 (VLAN classification) from the allowed rule type list on port ge.1.5. Any other allowed rule types on the port will still remain assigned to that port:

```
Matrix(rw)->set policy allowed-type ge.1.5 traffic-rule 27 clear
```

clear policy allowed-type

Use this command to clear the list of traffic rules currently assigned to the admin profile for one or more ports. This will reassign the default setting, which is all rules are allowed.

Syntax

clear policy allowed-type *port-string*

Parameters

port-string	Specifies port(s) on which to clear traffic rules.

Defaults

None.

Mode

Switch command, Read-Write.

Usage

This command will reassign the default setting, which is all rules are allowed.

Example

This example shows how to clear the allowed rule list from port ge.1.5:

```
Matrix(rw)->clear policy allowed-type ge.1.5
```

clear policy port-hit

Use this command to clear rule port hit indications on one or more ports.

Syntax

clear policy port-hit {**all** | **port-list** *port-list*}

Parameters

all | **port-list** *port-list*	Clears port hit indications on all ports or on one or more specified ports.

Downloaded from www.Manualslib.com manuals search engine

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to clear rule port hit indications on all ports:

```
Matrix(rw)->clear policy port-hit all
```


Downloaded from www.Manualslib.com manuals search engine

Configuring Policy Class of Service (CoS)

Using Port-Based or Policy-Based CoS Settings

Note: It is recommended that you use Enterasys NetSight Policy Manager as an alternative to CLI for configuring policy-based CoS on the Enterasys Matrix Series devices.

The Enterasys Matrix Series device supports Class of Service (CoS), which allows you to assign mission-critical data to higher priority through the device by delaying less critical traffic during periods of congestion. The higher priority traffic through the device is serviced first before lower priority traffic. The Class of Service capability of the device is implemented by a priority queueing mechanism. Class of Service is based on the IEEE 802.1D (802.1p) standard specification, and allows you to define eight priorities (0-7, with 7 granted highest priority) and, depending on port type, up to 16 transmit queues (0-15) of traffic for each port.

Enterasys Networks' enhanced CoS implementation allows you to use the following methods to configure Class of Service on the Enterasys Matrix Series device:

- Allowing the device to automatically assign policy-based inbound rate limiters and transmit queues as described in this section.
- Configuring transmit queueing and rate limiting on a per-port basis as described in Chapter 22.

By defult, policy-based CoS is disabled on the device, and default or user-assigned port-based 802.1D (802.1p) settings are used to determine transmit queues and traffic rate limiting. When policy-based CoS is enabled, the default and user-assigned settings will override port-based settings described in Chapter 22.

About Policy-Based CoS Default and User-Defined Configurations

Once enabled using the **set cos state** command as described in "set cos state" on page 8-23, the policy-based CoS function provides the following default configuration:

- Transmit queues (TXQ) — A strict-priority queueing mechanism which gives higher priority queues absolute preferential treatment over low priority queues. This ensures the transmit port does not serve a transmit queue unless all higher priority queues are empty. As described previously in this section, eight priority designations and, depending on port type, up to 16 four transmit queues are defined for each port.
- Inbound rate limiting (IRL) — No inbound rate limiters are configured.

You can add to these default configurations by defining new port groupings, and assigning inbound rate limiters or transmit queues and priorities. Whether you are specifying IRL or TXQ parameters, the process for user-defined CoS configuration involves the following steps and associated commands listed in Table 8-4.

Table 8-4 Configuring User-Defined CoS

To do this....	Use these commands...
Enable CoS.	**set cos state**
If desired, create new or change existing CoS port configurations.	**set cos port-config irl** **set cos port config txq**

Downloaded from www.Manualslib.com manuals search engine

Table 8-4 Configuring User-Defined CoS

To do this....	Use these commands...
Define IRL or TXQ resources (data rates or transmit priorities).	**set cos port-resource irl** **set cos port-resource txq**
Bind a CoS reference index ID to a defined resource.	**set cos reference irl** **set cos reference txq**
Bind an IRL or TXQ reference ID to a CoS setting index ID.	**set cos setting**
Associate CoS index IDs to policy rules.	**set policy rule**

Purpose

To configure policy-based Class of Service.

Commands

For information about...	Refer to page...
show cos state	8-23
set cos state	8-23
show cos port-type	8-24
show cos unit	8-26
show cos port-config	8-27
set cos port-config irl	8-28
clear cos port-config irl	8-29
set cos port-config txq	8-29
clear cos port-config txq	8-30
show cos port-resource	8-31
set cos port-resource irl	8-32
clear cos port-resource irl	8-33
set cos port-resource txq	8-33
clear cos port-resource txq	8-34
show cos reference	8-35
set cos reference irl	8-36
clear cos reference irl	8-36
set cos reference txq	8-37
clear cos reference txq	8-37
show cos settings	8-38
set cos settings	8-39
clear cos settings	8-39
show cos violation irl	8-40

Downloaded from www.Manualslib.com manuals search engine

For information about...	Refer to page...
clear cos violation irl	8-40
clear cos all-entries	8-41

show cos state

Use this command to display the Class of Service enable state.

Syntax

show cos state

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Only.

Example

This example shows how to show the Class of Service enable state:

```
Matrix(rw)->show cos state
Class-of-Service application is enabled
```

set cos state

Use this command to enable or disable Class of Service.

Syntax

set cos state{**enable** | **disable**}

Parameters

enable | **disable**	Enables or disables Class of Servic.e

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to enable Class of Service:

```
Matrix(rw)->set cos state enable
```


Downloaded from www.Manualslib.com manuals search engine

show cos port-type

Use this command to display Class of Service port type configurations.

Syntax

show cos port-type [**irl** | **txq**] [*index-list*]

Parameters

irl | **txq**	(Optional) Displays inbound rate limiting or transmit queue information.
index-list	(Optional) Displays information for a specific port type.

Defaults

If not specified, all rate limiting information for all port types will be displayed.

Mode

Switch command, Read-Only.

Usage

The Enterasys Matrix Series CoS implementation provides two default port type groupings for designating available rate limiting and transmit queue resources on device modules. Port type 0 designates one of 7GR4270-12, 7G4270-12, 7G4270-09, or 7G4270-10 DFE modules. Port type 1 designates all other modules, including DFE-Gold and NSA modules. Other port groupings can be configured using the commands in this section.

Example

This example shows how to display all Class of Service port type information. In this case, no new port groups have been configured, so information for the two device default groups of 0 and 1 are shown:

```
Matrix(rw)->show cos port-type
Number of resources:              Supported rate types:
 txq = transmit queue(s)           perc  = percentage
 irl = inbound rate limiter(s)     pps   = packets per second
 orl = outbound rate limiter(s)    Kbps  = kilobits per second
                                   Mbps  = megabits per second
                                   Gbps  = gigabits per second
                                   Tbps  = terabits per second

                     Number of
                     slices /
       Port type     Number of  Supported  Eligible          Unselected
Index  description   queues     rate type  ports             ports
-----  ------------  ---------  ---------  ----------------  --------------
0      DFE-P 16Q       64/16    perc       ge.1.1-12         ge.1.1-12
                                Kbps
                                Mbps
```


Downloaded from www.Manualslib.com manuals search engine

```
                                  Gbps

1       DFE-P 4Q         32/4     perc       ge.2.1-30;          ge.2.1-30;
                                  Kbps       ge.3.1-30;          ge.3.1-30;
                                  Mbps       ge.4.1-30;          ge.4.1-30;
                                  Gbps       fe.6.1-48;          fe.6.1-48;
                                             ge.6.1-6;           ge.6.1-6;
                                             fe.7.1-72           fe.7.1-72

        Port type      Number of  Supported  Eligible            Unselected
Index   description    limiters   rate type  ports               ports
-----   ------------   ---------  ---------  ------------------  --------------
0       DFE-P 32 IRL    32 irl    perc       ge.1.1-12           ge.1.1-12
                                  Kbps
                                  Mbps
                                  Gbps

1       DFE-P 8 IRL      8 irl    perc       ge.2.1-30;          ge.2.1-30;
                                  Kbps       ge.3.1-30;          ge.3.1-30;
                                  Mbps       ge.4.1-30;          ge.4.1-30;
                                  Gbps       fe.6.1-48;          fe.6.1-48;
                                             ge.6.1-6;           ge.6.1-6;
                                             fe.7.1-72           fe.7.1-72
```

Table 8-5 provides an explanation of the command output.

Table 8-5 show cos port-type Output Details

Output...	What it displays...
Index	Port type index. Port type 0 designates 7GR4270-12, 7G4270-12, 7G4270-09, and 7G4270-10 DFE modules only, and port type 1 designates all other modules.
Port type description	Resource-specific text description of the port type. Default names are: • DFE-P 16Q for port type 0 TXQ (Applies to 7GR4270-12, 7G4270-12, 7G4270-09, and 7G4270-10 DFE modules only). Port type 1 designates all other modules. • DFE-P or DFE-G 4Q for port type 1 TXQ • DFE-P 32 IRL for port type 0 IRL (Applies to 7GR4270-12, 7G4270-12, 7G4270-09, and 7G4270-10 DFE modules only). • DFE-P or DFE-G 8 IRL for port type 1 IRL
Number of slices / Number of queues	The total number of slices of transmit resources that can be divided among port queues, and the total number of queues available. Default port type 0 (7GR4270-12, 7G4270-12, 7G4270-09, and 7G4270-10 DFE modules only). allows 64 slices for 16 queues. Default port type 1 (all other modules) allows 32 slices for 4 queues.
Number of limiters	Maximum number of inbound rate limiters configurable for each port type. When configured for IRL, default port type 0 (7GR4270-12, 7G4270-12, 7G4270-09, and 7G4270-10 DFE modules only). allows for 32, and default port type 1 (all other modules) allows for 8.

Downloaded from www.Manualslib.com manuals search engine

Table 8-5 show cos port-type Output Details

Output...	What it displays...
Supported rate types	Unit of measure supported by the port type.
Eligible ports	Which device ports meet this port type criteria.
Unselected ports	Which ports have not been assigned user-defined port configuration settings,

show cos unit

Use this command to display Class of Service units of measure information, including rate type, minimum and maximum limits of the port groups, and their respective granularity.

Syntax

show cos unit [**irl** | **txq**] [**port-type** *index*]

Parameters

irl | **txq**	(Optional) Displays inbound rate limiting or transmit queue information.
port-type *index*	(Optional) Displays information for a specific port type.
	Displays the unit of measure as percentage of total bandwidth, or kilobits, megabits, or gigabits per second.

Defaults

If not specified, all rate limiting information for all port types and CoS units of measure will be displayed.

Mode

Switch command, Read-Only.

Example

This example shows how to show all Class of Service IRL unit of measure information:

```
Matrix(rw)->show cos unit irl

Port Type  Type  Unit  Maximum Rate  Minimum Rate  Granularity
---------  ----  ----  ------------  ------------  -----------
0          irl   Gbps  10            1             1
0          irl   Mbps  10000         1             1
0          irl   Kbps  10000000      5121024       1
0          irl   perc  100           1             1
1          irl   Gbps  10            1             1
1          irl   Mbps  10000         1             1
1          irl   Kbps  10000000      5121024       1
1          irl   perc  100           1             1
```


Downloaded from www.Manualslib.com manuals search engine

show cos port-config

Use this command to display Class of Service port group configurations.

Syntax

show cos port-config [**irl** | **txq**] [*group-type-index*]

Parameters

irl | **txq**	(Optional) Displays inbound rate limiting or transmit queue information.
group-type-index	(Optional) Displays information for a specific port group/type index. Valid entries are in the form of **group.type**. Group can be 0-7, with 0 designating the default group, and 1-7 reserved for user-defined groups. Default port type values cannot be changed, and are 0 for the 7GR4270-12, 7G4270-12, 7G4270-09, and 7G4270-10 DFE modules only, and 1 for all other modules.

Defaults

If not specified, all rate limiting information for all port types will be displayed.

Mode

Switch command, Read-Only.

Example

This example shows how to show all Class of Service port group configuration information:

```
Matrix(rw)->show cos port-config
* Percentage/queue (if any) are approximations based on
   [(slices/queue) / total number of slices]

Transmit Queue Port Configuration Entries
--------------------------------------------------------------------------
Port Group Name  :DFE-P 16Q
Port Group       :0
Port Type        :0
Assigned Ports   :ge.1.1-12
Arbiter Mode     :Strict
Slices/queue     :Q [ 0]:   0  Q [ 1]:   0  Q [ 2]:   0  Q [ 3]:   0
                 :Q [ 4]:   0  Q [ 5]:   0  Q [ 6]:   0  Q [ 7]:   0
                 :Q [ 8]:   0  Q [ 9]:   0  Q [10]:   0  Q [11]:   0
                 :Q [12]:   0  Q [13]:   0  Q [14]:   0  Q [15]:  64
Percentage/queue :Q [ 0]:   0% Q [ 1]:   0% Q [ 2]:   0% Q [ 3]:   0%
                 :Q [ 4]:   0% Q [ 5]:   0% Q [ 6]:   0% Q [ 7]:   0%
                 :Q [ 8]:   0% Q [ 9]:   0% Q [10]:   0% Q [11]:   0%
                 :Q [12]:   0% Q [13]:   0% Q [14]:   0% Q [15]: 100%
--------------------------------------------------------------------------
Port Group Name  :DFE-P 4Q
```


Downloaded from www.Manualslib.com manuals search engine

```
Port Group       :0
Port Type        :1
Assigned Ports   :ge.2.1-30;ge.3.1-30;ge.4.1-30;fe.6.1-48;ge.6.1-6;fe.7.1-72
Arbiter Mode     :Strict
Slices/queue     :Q [ 0]:   0  Q [ 1]:   0  Q [ 2]:   0  Q [ 3]:  32
Percentage/queue :Q [ 0]:   0% Q [ 1]:   0% Q [ 2]:   0% Q [ 3]: 100%
------------------------------------------------------------------------

Inbound Rate Limiting Port Configuration Entries
------------------------------------------------------------------------
Port Group Name  :DFE-P 32 IRL
Port Group       :0
Port Type        :0
Assigned Ports   :ge.1.1-12
------------------------------------------------------------------------
Port Group Name  :DFE-P 8 IRL
Port Group       :0
Port Type        :1
Assigned Ports   :ge.2.1-30;ge.3.1-30;ge.4.1-30;fe.6.1-48;ge.6.1-6;fe.7.1-72
------------------------------------------------------------------------
```

set cos port-config irl

Use this command to set the Class of Service inbound rate limiting port group configuration:

Syntax

set cos port-config irl *group-type-index* [**name** *name*] [**ports** *port-list*] [**append**] | [**clear**]

Parameters

group-type-index	Specifies an inbound rate limiting port group/type index for this entry. Valid entries are in the form of **group.type**. Group can be 0-7, with 0 designating the default group, and 1-7 reserved for user-defined groups. Default port type values cannot be changed, and are 0 for the 7GR4270-12, 7G4270-12, 7G4270-09, and 7G4270-10 DFE modules only, and 1 for all other modules.
name *name*	(Optional) Specifies a name for this configuration.
ports *port-list*	(Optional) Applies this configuration to one or more ports in the port group.
append | **clear**	(Optional) Appends or clears port designations from a previously configured port group.

Defaults

- If a **name** is not specified, default names described in Table 8-5 will be applied.
- If not specified, this configuration will be applied to all ports in the port group.
- If **append** or **clear** are not specified, port(s) will be appended to the specified port grouping.

Downloaded from www.Manualslib.com manuals search engine

Mode

Switch command, Read-Write.

Example

This example shows how to create a CoS inbound rate limiting port group entry named “test irl” with a port group ID of 1 and a port type ID of 1:

```
Matrix(rw)->set cos port-config irl 1.1 name test irl
```

clear cos port-config irl

Use this command to clear a non-default Class of Service inbound rate limiting port group configuration:

Syntax

clear cos port-config irl all | *group-type-index* {[**entry**] | [**name**] | [**ports**]}

Parameters

all | *group-type-index*	Clears all inbound rate limiting non-default configurations, or those for a specific user-defined port group index.
entry | **name** | **ports**	Deletes a specific entry or name, or clears the ports assigned to this inbound rate limiting configuration.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to delete the CoS inbound rate limiting port group entry 1.1:

```
Matrix(rw)->clear cos port-config irl 1.1 entry
```

set cos port-config txq

Use this command to set the Class of Service transmit queue port group configuration:

Syntax

set cos port-config txq *group-type-index* [**name** *name*] [**ports** *port-list*] [**append**] | [**clear**]

Downloaded from www.Manualslib.com manuals search engine

Parameters

group-type-index	Specifies a transmit queue port group/type index for this entry. Valid entries are in the form of **group.type**. Group can be 0-7, with 0 designating the default group, and 1-7 reserved for user-defined groups. Default port type values cannot be changed, and are 0 for the 7GR4270-12, 7G4270-12, 7G4270-09, and 7G4270-10 DFE modules only, and 1 for all other modules.
name *name*	(Optional) Specifies a name for this configuration.
ports *port-list*	(Optional) Applies this configuration to one or more ports in the port group.
append | **clear**	(Optional) Appends or clears port designations from a previously configured port group.

Defaults

- If a **name** is not specified, default names described in Table 8-5 will be applied.
- If not specified, this configuration will be applied to all ports in the port group.
- If **append** or **clear** are not specified, port(s) will be appended to the specified port grouping.
- If **arb-slice** or **arb-percentage** values are not specified, default allocations will be applied.

Mode

Switch command, Read-Write.

Example

This example shows how to create a CoS transmit queue port group entry named “test txq” with a port group ID of 2 and a port type ID of 1:

```
Matrix(rw)->set cos port-config txq 2.1 name test txq
```

clear cos port-config txq

Use this command to clear one or all non-default Class of Service transmit queue port group configurations:

Syntax

clear cos port-config txq all | *group-type-index* {**entry** | **name** | **ports** }

Parameters

all | *group-type-index*	Clears all transmit queue port config entries or a specific entry.
entry	Clears all non-default transmit queue entries.
name	Clears the name associated with this transmit queue entry.
ports	Clears the port(s) assigned to this port group.

Defaults

None.

Downloaded from www.Manualslib.com manuals search engine

Mode

Switch command, Read-Write.

Example

This example shows how to clear all non-default CoS transmit queue port group entries:

```
Matrix(rw)->clear cos port-config txq all
```

show cos port-resource

Use this command to display Class of Service port resource configuration information.

Syntax

show cos port-resource irl *group-type-index* [*resource*] [**violators**]

Parameters

irl | **txq**	(Optional) Displays inbound rate limiting or transmit queue information.
group-type-index	(Optional) Displays information for a specific port group/type entry.
resource	(Optional) Displays rate limiters or transmit queues associated with this entry.
violators	(Optional) Displays ports that have violated inbound rate limiters.

Defaults

If no options are specified, all rate limiting information for all port types will be displayed.

Mode

Switch command, Read-Only.

Example

This example shows how to show all inbound rate limiting port resource configuration information for port group 0.1:

```
Matrix(rw)->show cos port-resource irl 0.1
'?' after the rate value indicates an invalid rate value

Group Index Resource Type Unit    Rate      Rate Limit Type Action
----------- -------- ---- ---- ----------   --------------- -----
0.1         0        irl  perc none         drop            none
0.1         1        irl  perc none         drop            none
0.1         2        irl  perc none         drop            none
0.1         3        irl  perc none         drop            none
0.1         4        irl  perc none         drop            none
0.1         5        irl  perc none         drop            none
0.1         6        irl  perc none         drop            none
0.1         7        irl  perc none         drop            none
```


Downloaded from www.Manualslib.com manuals search engine

set cos port-resource irl

Use this command to configure a Class of Service inbound rate limiting port resource entry.

Syntax

set cos port-resource irl *group-type-index irl-number* {[**unit** {**percentage** | **kbps** | **mbps** | **gbps**}] [**rate** *rate*] [**type** {**drop**}] [**syslog** {**disable** | **enable**}] [**trap** {**disable** | **enable**}] [**disable-port** {**disable** | **enable**}]}

Parameters

group-type-index	Specifies an inbound rate limiting port group/type index for this entry. Valid entries are in the form of **group.type**. Group can be 0-7, with 0 designating the default group, and 1-7 reserved for user-defined groups. Default port type values cannot be changed, and are 0 for the 7GR4270-12, 7G4270-12, 7G4270-09, and 7G4270-10 DFE modules, and 1 for all other modules.
irl-number	Specifies an inbound rate limiter ID to be associated with this entry.
unit percentage | **kbps** | **mbps** | **gbps**	Specifies the unit of measure as percentage of total bandwidth, or kilobits, megabits, or gigabits per second.
rate *rate*	(Optional) Data rate in units for this inbound rate limiter.
type drop	(Optional) Specifies that frames exceeding this limiter will be dropped.
syslog disable | **enable**	(Optional) Enables or disables the generation of a Syslog message when this limiter is exceeded.
trap disable | **enable**	(Optional) Enables or disables the sending of an SNMP trap message when this limiter is exceeded.
disable-port disable | **enable**	(Optional) Enables or disables the disabling of the violating port when this limiter is exceeded.

Defaults

- If a **rate** is not specified, port defaults will be applied.
- If not specified, frames will not be dropped.
- If not specified, Syslog and port disabling will not be configured.

Mode

Switch command, Read-Write.

Example

This example shows how to configure Class of Service port resource IRL entry 0 for port group 0.1 assigning an inbound rate limit of 512 kilobits per second This entry will trigger a Syslog and an SNMP trap message if this rate is exceeded:

```
Matrix(rw)->set cos port-resource irl 0.1 0 unit kbps 512 syslog enable trap enable
```


Downloaded from www.Manualslib.com manuals search engine

clear cos port-resource irl

Use this command to clear one or all Class of Service inbound rate limiting port resource configurations:

Syntax

clear cos port-resource irl all | *group-type-index resource* [**unit**] [**rate**] [**type**] [**syslog**] [**trap**] [**disable-port**] [**violators** *port-list*]

Parameters

all | *group-type-index*	Clears all inbound rate limiting port resource entries or a specific entry.
resource	Specifies a resource entry to be cleared.
unit	(Optional) Clears the unit of measure setting.
rate	(Optional) Clears the data rate setting.
type	(Optional) Clears the type of action setting.
syslog	(Optional) Clears the Syslog setting.
trap	(Optional) Clears the SNMP trap setting.
disable-port	(Optional) Clears the disable port setting.
violators *port-list*	(Optional) Clears the limit violation setting.

Defaults

If no options are specified, all non-default settings will be cleared for the associated rate limiter.

Mode

Switch command, Read-Write.

Example

This example shows how to clear all inbound rate limiting settings associated with port group 0.1, resource entry 0:

```
Matrix(rw)->clear cos port-resource irl 0.1 0
```

set cos port-resource txq

Use this command to configure a Class of Service transmit queue port resource entry.

Syntax

set cos port-resource txq *group-type-index transmit-queue* {[**unit** {**percentage** | **kbps** | **mbps** | **gbps**}] [**rate** *rate*] [**algorithm** {**tail-drop**}]}

Downloaded from www.Manualslib.com manuals search engine

Parameters

group-type-index	Specifies a transmit queue port group/type index for this entry. Valid entries are in the form of **group.type**. Group can be 0-7, with 0 designating the default group, and 1-7 reserved for user-defined groups. Default port type values cannot be changed, and are 0 for the 7GR4270-12, 7G4270-12, 7G4270-09, and 7G4270-10 DFE modules, and 1 for all other modules.
transmit-queue	Specifies a transmit queue to be associated with this entry. Valid values are 0-7.
unit percentage | **kbps** | **mbps** | **gbps**	Specifies the unit of measure as percentage of total bandwidth, or kilobits, megabits, or gigabits per second.
rate *rate*	(Optional) Specifies a data rate in units for this transmit queue.
algorithm tail-drop	(Optional) Sets the algorithm by which transmit frames are discarded as discarding frames from the tail of the queue.

Defaults

- If a **rate** is not specified, port defaults will be applied.
- If not specified, no algorithm will be assigned.

Mode

Switch command, Read-Write.

Example

This example shows how to configure a Class of Service port resource entry for port group 0.1 assigning 50 percent of the total available inbound bandwidth to transmit queue 7:

```
Matrix(rw)->set cos port-resource txq 0.1 7 unit percentage 50
```

clear cos port-resource txq

Use this command to clear one or all Class of Service transmit queue port resource entry.

Syntax

clear cos port-resource txq all | *group-type-index resource*[**unit**] [**rate**] [**algorithm**]

Parameters

all | *group-type-index*	Clears all transmit queue port resource entries or a specific entry.
resource	Specifies a resource entry to be cleared.
unit	(Optional) Clears unit of measure settings.
rate	(Optional) Clears rate settings.
algorithm tail-drop	(Optional) Clears algorithm settings.

Defaults

If no options are specified, all associated non-default settings will be cleared.

Downloaded from www.Manualslib.com manuals search engine

Mode

Switch command, Read-Write.

Example

This example shows how to clear all port resource settings associated with Class of Service transmit queue 1 in port group 0.1:

```
Matrix(rw)->clear cos port-resource txq 0.1 1
```

show cos reference

Use this command to display Class of Service port reference information.

Syntax

show cos reference [**txq** | **irl** *group-type-index* [*reference*]]

Parameters

irl | **txq**	(Optional) Displays inbound rate limiting or transmit queue reference information.
group-type-index	(Optional) Displays information for a specific port group/type entry.
reference	(Optional) Displays information for a specific reference entry.

Defaults

If no options are specified, all reference information for all port types will be displayed.

Mode

Switch command, Read-Only.

Example

This example shows how to show all transmit queue reference configuration information for port group 0.1:

```
Matrix(rw)->show cos reference txq 0.1
Group Index Reference Type    Queue
----------- --------- ---- ------------
0.1         0         txq  0
0.1         1         txq  0
0.1         2         txq  0
0.1         3         txq  0
0.1         4         txq  1
0.1         5         txq  1
0.1         6         txq  1
0.1         7         txq  1
0.1         8         txq  2
0.1         9         txq  2
0.1         10        txq  2
0.1         11        txq  2
```


Downloaded from www.Manualslib.com manuals search engine

```
0.1          12          txq  3
0.1          13          txq  3
0.1          14          txq  3
0.1          15          txq  3
```

set cos reference irl

Use this command to set a Class of Service inbound rate limiting reference configuration.

Syntax

set cos reference irl *group-type-index reference* **rate-limit** *number*

Parameters

group-type-index	Specifies an inbound rate limiting port group/type index for this entry. Valid entries are in the form of **group.type**. Group can be 0-7, with 0 designating the default group, and 1-7 reserved for user-defined groups. Default port type values cannot be changed, and are 0 for the 7GR4270-12, 7G4270-12, 7G4270-09, and 7G4270-10 DFE modules, and 1 for all other modules.
reference	Specifies a reference number to be associated with this entry.
rate-limit *number*	Specifies a rate limiter resource ID to bind to this entry.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to configure inbound rate limiting reference entry 0 for port group 0.1 referencing resources defined by IRL entry 0:

```
Matrix(rw)->set cos reference irl 0.1 0 rate-limit 0
```

clear cos reference irl

Use this command to clear one or all Class of Service inbound rate limiting reference configurations.

Syntax

clear cos reference irl {**all** | *group-type-index reference*}

Parameters

all | *group-type-index*	Clears all non-default inbound rate limiting reference entries or a specific entry.
reference	Specifies a reference number of the entry to be cleared.

Downloaded from www.Manualslib.com manuals search engine

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to clear all Class of Service inbound rate limiting reference entries:

```
Matrix(rw)->clear cos reference irl all
```

set cos reference txq

Use this command to set a Class of Service inbound rate limiting reference configuration.

Syntax

set cos reference txq *group-type-index reference* **queue** *number*

Parameters

group-type-index	Specifies a transmit queue port group/type index for this entry. Valid entries are in the form of **group.type**. Group can be 0-7, with 0 designating the default group, and 1-7 reserved for user-defined groups. Default port type values cannot be changed, and are 0 for the 7GR4270-12, 7G4270-12, 7G4270-09, and 7G4270-10 DFE modules, and 1 for all other modules.
reference	Specifies a reference number to be associated with this entry.
queue *number*	Specifies a transmit queue resource ID to bind to this entry.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to configure inbound rate limiting reference resource entry 0 for port group 0.1 referencing resources defined by TXQ entry 0:

```
Matrix(rw)->set cos reference irl 0.1 0 queue 0
```

clear cos reference txq

Use this command to clear one or all non-default Class of Service transmit queue reference configurations.

Syntax

clear cos reference txq {**all** | *group-type-index reference*}

Downloaded from www.Manualslib.com manuals search engine

Parameters

all | *group-type-index*	Clears all non-default transmit queue reference entries or a specific entry.
reference	Specifies a reference number of the entry to be cleared.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to clear all Class of Service transmit queue reference entries:

```
Matrix(rw)->clear cos reference txq all
```

show cos settings

Use this command to display Class of Service parameters.

Syntax

show cos settings [*cos-list*]

Parameters

cos-list	(Optional) Specifies a Class of Service entry to display.

Defaults

If not specified, all CoS entries will be displayed.

Mode

Switch command, Read-Only.

Example

This example shows how to show all CoS settings:

```
Matrix(rw)->show cos settings
* Means attribute has not been configured

CoS Index  Priority    ToS      TxQ    IRL
---------  ----------  -------  -----  -----
0          0           *        0      *
1          1           *        2      *
2          2           *        4      *
3          3           *        6      *
4          4           *        8      *
5          5           *        10     *
```


Downloaded from www.Manualslib.com manuals search engine

```
6          6          *          12     *
7          7          *          14     *
```

set cos settings

Use this command to configure a Class of Service entry.

Syntax

set cos settings *cos-list* [**priority** *priority*] [**tos-value** *tos-value*] [**txq-reference** *txq-reference*] [**irl-reference** *irl-reference*]

Parameters

cos-list	Specifies a Class of Service entry. Valid values are 0 - 255.
priority *priority*	(Optional) Specifies a CoS priority value. Valid values are **0** - **7**, with 0 being the lowest priority.
tos-value *tos-value*	(Optional) Specifies a Type of Service value with mask in the format of 0 - 255:0 - 255 or 0 - 0xFF:0 - 0xFF.
txq-reference *txq-reference*	(Optional) Specifies the transmit queue associated with this entry. Valid values are 0 - 15
irl-reference *irl-reference*	(Optional) Specifies the inbound rate limiter associated with this entry. Valid values are 0 - 31.

Defaults

If no optional parameters are specified, none will be applied.

Mode

Switch command, Read-Write.

Example

This example shows how to create CoS entry 2 with a priority value of 3 and bind it to transmit queue reference ID 5:

```
Matrix(rw)->set cos settings 2 priority 3 txq-reference 5
```

clear cos settings

Use this command to clear Class of Service entry settings.

Syntax

clear cos settings *cos-list* {[**all**] | [**priority**] [**tos-value**] [**txq-reference**] [**irl-reference**]}

Parameters

cos-list	Specifies a Class of Service entry to clear.
all	Clears all settings associated with this entry.
priority	Clears the priority value associated with this entry.

Downloaded from www.Manualslib.com manuals search engine

tos-value	Clears the Type of Service value associated with this entry.
txq-reference	Clears the transmit queue reference associated with this entry.
irl-reference	Clears the inbound rate limiting reference associated with this entry.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to clear the priority and transmit queue reference values for CoS entry 2:

```
Matrix(rw)->clear cos settings 2 priority txq-reference
```

show cos violation irl

Use this command to display Class of Service violation configurations.

Syntax

show cos violation irl [*violation-index*]

Parameters

violation-index	(Optional) Displays information for a specific violation index. Valid entries are in the form of *port-list*:*irl-lis*t, or ***.*.*:*** for all entries.

Defaults

If no options are specified, all inbound rate limiting violation information will be displayed.

Mode

Switch command, Read-Only.

Example

This example shows how to show any CoS inbound rate limiting violations:

```
Matrix(rw)->show cos violation irl
There are no ports disabled by any irl rate limiters
```

clear cos violation irl

Use this command to clear Class of Service inbound rate limiting violation configurations.

Syntax

clear cos violation irl {**all** | **disabled-ports** | *violation-index*} {**both** | **status** | **counter**}

Downloaded from www.Manualslib.com manuals search engine

Parameters

all	Clears all inbound rate limiting violation entries.
disabled-ports	Clears the list of ports that are disabled because of violating an inbound rate limiter.
violation-index	Clears the entry for a specific violation index.
both | **status** | **counter**	Clears the violation status, the violation counter, or both.

Defaults

If no options are specified, all information for all types of CoS violations will be displayed.

Mode

Switch command, Read-Write.

Example

This example shows how to clear both status and counters from all CoS inbound rate limiting violation entries:

```
Matrix(rw)->clear cos violation irl all both
```

clear cos all-entries

Use this command to clears all Class of Service entries except priority settings 0 - 7.

Syntax

clear cos all-entries

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to clear all Class of Service entries except priority settings 0 - 7:

```
Matrix(rw)->clear cos all-entries
```


Downloaded from www.Manualslib.com manuals search engine

Configuring Policy-Based Routing



Router: These commands can be executed when the device is in **router mode** only. For details on how to enable router configuration modes, refer to “Enabling Router Configuration Modes” on page 2-103.

About Policy-Based Routing

Normally, IP packets are forwarded according to the route that has been selected by traditional routing protocols, such as RIP and OSPF, or by static routes. In this case, selection is performed based only on the destination of the IP packet. Policy-based routing adds more flexibility to routing by specifying other alternative paths. When a route map list is configured and applied to an interface, policy-based routing will check an incoming IP packet against the access list (ACL) of each map of that list in sequence. If no ACL permit rule matches the packet, the packet is forwarded on the normal routing path using a route lookup. If a permit rule does match, the ACL check is exited and the map having the ACL matching the packet is checked for further routing instruction. If the action of that map is permit, and a next hop is specified, policy-based routing will forward the packet to the next hop specified in that map. Otherwise it will forward the packet on the normal routing path using a route lookup. One route map list is allowed per routing interface.

Purpose

To review and configure route maps and policy-based routing.

Commands

For information about...	Refer to page...
show route-map	8-42
route-map	8-43
match ip address	8-44
set next hop	8-45
show ip policy	8-45
ip policy route-map	8-46
ip policy priority	8-47
ip policy load-policy	8-48
ip policy pinger	8-48

show route-map

Use this command to display a configured route map list for policy-based routing.

Syntax

show route-map *id-number*

Downloaded from www.Manualslib.com manuals search engine

Parameters

id-number	Specifies the ID number for which to display a configured PBR route map list. Valid values for PBR are **100** - **199**.

Defaults

None.

Mode

Router command, Global configuration: **Matrix>Router(config)#**

Example

This example shows how to display route map list 101. In this case, the packet source IP addresses matching ACL lists 2,3,4,8, or 110 will be forwarded to next hop 10.2.1.1, 10.2.2.1 or 10.2.3.1. The route map list was created using the **route-map** command ("route-map" on page 8-43). The packet source IP address was then matched to an ACL using the **match ip address** command ("match ip address" on page 8-44), and the packet's next hops were defined using the **set next-hop** command ("set next hop" on page 8-45):

```
Matrix>Router#show route map 101
route-map 101, permit, sequence 1
 Match clauses:
  ip address 2 3 4 8 110
Set clauses:
  next-hop 10.2.1.1 10.2.2.1 10.2.3.1
 Policy matches: 0 packets
```

route-map

Use this command to create a route map for policy-based routing and to enable policy-based routing configuration mode.

Syntax

route-map *id-number* [**permit** | **deny**] [*sequence-number*]

no route-map *id-number*

Parameters

id-number	Specifies a route map list ID number to which this route map will be added. If an unused ID number is specified, a new route map list will be created. Valid values are for policy-based routing are: **100** - **199**.
permit	(Optional) Permits the packet to bypass route lookup and be forwarded to the next hop configured in the matching route map.
deny	(Optional) Denies policy-based routing, forcing the packet to continue on its normal routing path.
sequence-number	(Optional) Specifies the order of this map in the route map list, and the order in which this route map will be checked for matching access list criteria. The packet check will exit with the first map in the list which matches the packet data.

Downloaded from www.Manualslib.com manuals search engine

Defaults

- If **permit** or **deny** is not specified, this command will enable route map or policy based routing configuration mode.
- If *sequence-number* is not specified, **10** will be applied.

Mode

Router command, Global configuration: **Matrix>Router(config)#**

Usage

Use this command to add a route map to an existing route map list by specifying the list's *id-number* and a new *sequence-number*.

The "no" form of this command removes the specified route map list:.

Example

This example shows how to create route map 101 with a sequence order of 20:

```
Matrix>Router(config)#route-map 101 permit 20
```

match ip address

Use this command to match a packet source IP address against a PBR access list. Up to 5 access lists can be matched.

Syntax

match ip address *access-list-number*

no match ip address *access-list-number*

Parameters

ip address	Matches packet source IP addresses to the specified access list.
access-list-number	Specifies an access list to match to the packet source IP address. Valid values are **1** - **199**.

Defaults

None.

Mode

Policy-based routing configuration: **Matrix>Router(config-route-map-pbr)#**

Usage

The "no" form of this command removes the match between an access list and this route map.

Example

This example shows how to match a packet source IP address to access list 1:

```
Matrix>Router(config)#route-map 101 Matrix>Router(config-route-map-pbr)#match ip
address 1
```


Downloaded from www.Manualslib.com manuals search engine

set next hop

Use this command to set one or more next hop IP address for packets matching an extended access list in a configured route map.

Syntax

set next hop {*next-hop1*}[*next-hop2....next-hop5*]

no set next hop {*next-hop1*}[*next-hop2....next-hop5*]

Parameters

next-hop	Specifies a next hop IP address(es). Up to five can be configured.

Defaults

None.

Mode

Router command, Policy-based routing configuration: **Matrix>Router(config-route-map-pbr)#**

Usage

The "no" form of this command deletes next hop IP address(es).

Example

This example shows how to set IP address 10.2.3.4 as the next hop for packets matching ACL 1:

```
Matrix>Router(config)#route-map 101 permit 20
Matrix>Router(config-route-map-pbr)#match ip address 1
Matrix>Router(config-route-map-pbr)#set next-hop 10.2.3.4
```

show ip policy

Use this command to display the policy applied to a routing interface.

Syntax

show ip policy

Parameters

None.

Defaults

None.

Mode

Router command, Global configuration: **Matrix>Router(config)#**

Downloaded from www.Manualslib.com manuals search engine

Example

This example shows how to display policy information:

```
Matrix>Router(config)#show ip policy
Interface  Route map  Priority  Load policy        Pinger  Interval Retries
3          103        first     first-available    off     3        3
2          102        only      round-robin        on      10       4
```

Table 8-6 provides an explanation of the command output.

Table 8-6 show ip policy Output Details

Output...	What it displays...
Interface	Routing interface.
Route map	Route map assigned to the routing interface (using the **ip policy route-map** command as described in "ip policy route-map" on page 8-46.)
Priority	How the PBR next hop selection will be prioritized. Set with the **ip policy priority** command as described in "ip policy priority" on page 8-47.
Load policy	How the PBR next hop will be selected. Set with the **ip policy load-policy** command as described in "ip policy priority" on page 8-47.
Pinger	Whether PBR next hop pinging is on or off. Can be turned on and configured using the **ip policy pinger** command as described in "ip policy pinger" on page 8-48.
Interval	PBR next hop ping interval (in seconds). Default of 3 can be reset using the **ip policy pinger** command as described in "ip policy pinger" on page 8-48.
Retries	Number of PBR next hop ping retries. Default of 3 can be reset using the **ip policy pinger** command as described in "ip policy pinger" on page 8-48.

ip policy route-map

Use this command to assign a route map list to a routing interface**.**

Syntax

ip policy route-map *id-number*

no ip policy route-map

Parameters

id-number	Specifies a route map ID number. Valid values are **100** - **199**, and must match a value previously set using the **route-map** command ("route-map" on page 8-43). **Note:** Only one route map list is allowed per interface.

Defaults

None.

Downloaded from www.Manualslib.com manuals search engine

Mode

Router command, Interface configuration: **Matrix>Router(config-if(Vlan <vlan_id>))#**

Usage

The "no" form of un-assigns a route map list.

Example

This example shows how to assign route map 101 to VLAN 1:

```
Matrix>Router(config)#interface vlan 1
Matrix>Router(config-if(Vlan 1))#ip policy route-map 101
```

ip policy priority

Use this command to prioritize PBR next hop behavior**.**

Syntax

ip policy priority {[**only**] [**first**] [**last**]}

no ip policy priority

Parameters

only | **first** | **last**	Prioritizes use of the PBR configured policy — as opposed to doing a lookup in the FIB (Forward Information Base) route table for a next hop — as follows: • **only** - uses the PBR next hop, but if it is unavailable, drops the packet. • **first** (default) - uses the PBR next hop, but if unavailable, falls back to the FIB. • **last** - uses the FIB, but if no route is found, then uses the PBR next hop.

Defaults

None.

Mode

Router command, Interface configuration: **Matrix>Router(config-if(Vlan <vlan_id>))#**

Usage

The "no" form of this command resets the PBR priority configuration back to the default of **first**.

Example

This example shows how to set the IP policy priority on VLAN 1 to "last":

```
Matrix>Router(config)#interface vlan 1
Matrix>Router(config-if(Vlan 1))#ip policy priority last
```


Downloaded from www.Manualslib.com manuals search engine

ip policy load-policy

Use this command to configure PBR next hop behavior.

Syntax

ip policy load-policy {[**first-available**] [**round-robin**] [**ip-hash** {**sip** | **dip** | **both**}]}

no ip policy load-policy

Parameters

first-available | **round-robin** | **ip-hash sip** | **dip** | **both**	Specifies next hop selection behavior as: • **first-available** (default) - uses the first available next hop from the list of next hops • **round-robin -** circulates among the available next hops in the list. • **ip-hash sip** | **dip** | **both** - chooses a next hop based on a XOR hash of the IP source address, the IP destination address, or both.

Defaults

If **pinger** is not specified, none is configured.

Mode

Router command, Interface configuration: **Matrix>Router(config-if(Vlan <vlan_id>))#**

Usage

When more than one next hop is configured (using the **set next hop** command as described in "set next hop" on page 8-45) the load policy specifies choosing one next hop from among the sequence of next hops in the map matching the current packet. A next hop is considered available by default unless a pinger task is running and has flagged it as unavailable.

The "no" form of this command resets the next hop behavior to **first-available**.

Example

This example shows how to set the load policy behavior on VLAN 1 to "round-robin":

```
Matrix>Router(config)#interface vlan 1
Matrix>Router(config-if(Vlan 1))#ip policy load-policy round-robin
```

ip policy pinger

Use this command to configure behavior for pinging PBR next hops.

Syntax

ip policy pinger {**off** | **on** [**interval** *interval*] [**retries** *retries*}

no ip policy pinger

Parameters

off	Turns ping off so all next hops are available by default.
on	Starts pinging all next-hops in the route map list.

Downloaded from www.Manualslib.com manuals search engine

interval *interval*	(Optional) When ping is on, specifies the ping interval in seconds. Valid values are 1 - 30. Default is 3.
retries *retries*	(Optional) When ping is on, specifies the number of retries (timeout failures) before setting the hop as unavailable. Valid values are 1 - 10. Default is 3.

Defaults

- If not specified, **interval** will be set to 3 seconds.
- If not specified, **retries** will be set to 3.

Mode

Router command, Interface configuration: **Matrix>Router(config-if(Vlan <vlan_id>))#**

Usage

The “no” form of this command turns PBR ping to off.

Example

This example shows how to configure the PBR ping interval to 5 and retries to 4 on VLAN 1:

```
Matrix>Router(config)#interface vlan 1
Matrix>Router(config-if(Vlan 1))#ip policy pinger on interval 5 retries 4
```


Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

9

IGMP Configuration

This chapter describes the IGMP Configuration set of commands and how to use them.

For information about...	Refer to page...
About IP Multicast Group Management	9-1
IGMP Configuration Summary	9-2
Enabling / Disabling IGMP	9-2
Configuring IGMP	9-5

About IP Multicast Group Management

The Internet Group Management Protocol (IGMP) runs between hosts and their immediately neighboring multicast switch device. The protocol's mechanisms allow a host to inform its local switch device that it wants to receive transmissions addressed to a specific multicast group.

A multicast-enabled switch device can periodically ask its hosts if they want to receive multicast traffic. If there is more than one switch device on the LAN performing IP multicasting, one of these devices is elected "querier" and assumes the responsibility of querying the LAN for group members.

Based on the group membership information learned from IGMP, a switch device can determine which (if any) multicast traffic needs to be forwarded to each of its ports. At Layer-3, multicast switch devices use this information, along with a multicast routing protocol, to support IP multicasting across the Internet.

IGMP provides the final step in an IP multicast packet delivery service since it is only concerned with forwarding multicast traffic from the local switch device to group members on a directly attached subnetwork or LAN segment.

This switch device supports IP multicast group management by

- passively snooping on the IGMP query and IGMP report packets transferred between IP multicast switches and IP multicast host groups to learn IP multicast group members, and
- actively sending IGMP query messages to solicit IP multicast group members.

The purpose of IP multicast group management is to optimize a switched network's performance so multicast packets will only be forwarded to those ports containing multicast group hosts or multicast switch devices instead of flooding to all ports in the subnet (VLAN).

In addition to passively monitoring IGMP query and report messages, the Enterasys Matrix Series device can also actively send IGMP query messages to learn locations of multicast switches and member hosts in multicast groups within each VLAN.

Downloaded from www.Manualslib.com manuals search engine

However, note that IGMP neither alters nor routes any IP multicast packets. Since IGMP is not concerned with the delivery of IP multicast packets across subnetworks, an external IP multicast switch device is needed if IP multicast packets have to be routed across different subnetworks.

IGMP Configuration Summary

Multicasting is used to support real-time applications such as video conferences or streaming audio. A multicast server does not have to establish a separate connection with each client. It merely broadcasts its service to the network, and any hosts that want to receive the multicast register with their local multicast switch/router. Although this approach reduces the network overhead required by a multicast server, the broadcast traffic must be carefully pruned at every multicast switch/router it passes through to ensure that traffic is only passed to the hosts that subscribed to this service.

The Enterasys Matrix Series switch device uses IGMP (Internet Group Management Protocol) to query for any attached hosts who want to receive a specific multicast service. The device looks up the IP Multicast Group used for this service and adds any port that received a similar request to that group. It then propagates the service request on to any neighboring multicast switch/router to ensure that it will continue to receive the multicast service.

Enabling / Disabling IGMP

Purpose

To display IGMP information and to enable or disable IGMP snooping on the device.

Commands

For information about...	Refer to page...
show igmp enable	9-2
set igmp enable	9-3
set igmp disable	9-3

show igmp enable

Use this command to display the status of IGMP on one or more VLAN(s).

Syntax

show igmp enable *vlan-list*

Parameters

vlan-list	Specifies the VLAN(s) for which to display IGMP status.

Defaults

None.

Downloaded from www.Manualslib.com manuals search engine

Mode

Switch command, Read-Only.

Example

This example shows how to display the IGMP status for VLAN 104:

```
Matrix(rw)->show igmp enable 104
IGMP Default State for vlan 104 is Disabled
```

set igmp enable

Use this command to enable IGMP on one or more VLANs.

Syntax

set igmp enable *vlan-list*

Parameters

vlan-list	Specifies the VLAN(s) on which to enable IGMP.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to enable IGMP on VLAN 104:

```
Matrix(rw)->set igmp enable 104
```

set igmp disable

Use this command to disable IGMP on one or more VLANs.

Syntax

set igmp enable *vlan-list*

Parameters

vlan-list	Specifies the VLAN(s) on which to enable IGMP.

Defaults

None.

Mode

Switch command, Read-Write.

Downloaded from www.Manualslib.com manuals search engine

Example

This example shows how to disable IGMP on VLAN 104:

```
Matrix(rw)->set igmp disable 104
```


Downloaded from www.Manualslib.com manuals search engine

Configuring IGMP

Purpose

To display and set IGMP configuration parameters, including query interval and response time settings, and to create and configure static IGMP entries.

Commands

For information about...	Refer to page...
show igmp query	9-5
set igmp query-enable	9-6
set igmp query-disable	9-6
show igmp grp-full-action	9-7
set igmp grp-full-action	9-7
show igmp config	9-8
set igmp config	9-9
set igmp delete	9-10
show igmp groups	9-10
show igmp static	9-11
set igmp add-static	9-11
set igmp remove-static	9-12
show igmp protocols	9-13
set igmp protocols	9-13
clear igmp protocols	9-14
show igmp vlan	9-14
show igmp reporters	9-15
show igmp flows	9-16
show igmp counters	9-16
show igmp number-groups	9-17

show igmp query

Use this command to display the IGMP query status of one or more VLANs.

Syntax

show igmp query *vlan-list*

Parameters

vlan-list	Specifies the VLAN(s) for which to display IGMP query state.

Downloaded from www.Manualslib.com manuals search engine

Defaults

None.

Mode

Switch command, Read-Only.

Example

This example shows how to display the IGMP query state for VLAN 1:

```
Matrix(rw)->show igmp query 1
IGMP querying on vlan 1 is Disabled
```

set igmp query-enable

Use this command to enable IGMP querying on one or more VLANs.

Syntax

set igmp query-enable *vlan-list*

Parameters

vlan-list	Specifies the VLAN(s) on which to enable IGMP querying.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to enable IGMP querying on VLAN 104:

```
Matrix(rw)->set igmp query-enable 104
```

set igmp query-disable

Use this command to disable IGMP querying on one or more VLANs.

Syntax

set igmp query-disable *vlan-list*

Parameters

vlan-list	Specifies the VLAN(s) on which to disable IGMP querying.

Defaults

None.

Downloaded from www.Manualslib.com manuals search engine

Mode

Switch command, Read-Write.

Example

This example shows how to disable IGMP querying on VLAN 104:

```
Matrix(rw)->set igmp query-disable 104
```

show igmp grp-full-action

Use this command to show what action to take with multicast frames when the multicast IGMP group table is full

Syntax

show igmp grp-full-action

Defaults

None.

Mode

Switch command, Read-Only.

Example

This example shows how to display the action taken for multicast frames when the IGMP group table is full:

```
Matrix(rw)->show igmp grp-full-action
Group Table Full Action: Flood to Vlan
```

set igmp grp-full-action

Use this command to determine what action to take with multicast frames when the multicast group table is full.

Syntax

set igmp grp-full-action *action*

Parameters

action	Specifies the action to take when the multicast Group Table is full. The options are: • **1**-send multicast frames to Routers • **2**-flood multicast frames to the VLAN

Defaults

Flood multicast frames to the Vlan

Downloaded from www.Manualslib.com manuals search engine

Mode

Switch command, Read-Write.

Example

This example shows how to flood multicast frames to the VLAN when the multicast group table is full:

```
Matrix(rw)->set igmp grp-full-action 2
```

show igmp config

Use this command to display IGMP configuration information for one or more VLANs.

Syntax

show igmp config *vlan-list*

Parameters

vlan-list	Specifies the VLAN(s) for which to display IGMP configuration information.

Defaults

None.

Mode

Switch command, Read-Only.

Example

This example shows how to display IGMP configuration information for VLAN 1:

```
Matrix(rw)->show igmp config 1
IGMP config for vlan 1
VlanQueryInterval         - 125
VlanStatus                - Active
Vlan IGMP Version         - 2
VlanQuerier               - 134.141.22.1
VlanQueryMaxResponseTime  - 10
VlanRobustness            - 2
VlanLastMemberQueryIntvl  - 10
VlanQuerierUpTime         - 24039
```

Table 9-1 shows a detailed explanation of command output. For details on using the **set igmp config** command to set these parameters, refer to "set igmp config" on page 9-9.

Table 9-1 show igmp config Output Details

Output...	What it displays...
VlanQueryInterval	Frequency (in seconds) of host-query frame transmissions.
VlanStatus	Whether or not VLAN configuration is **Active** or **Not in Service**.

Downloaded from www.Manualslib.com manuals search engine

Table 9-1 show igmp config Output Details (continued)

Output...	What it displays...
Vlan IGMP Version	Whether or not IGMP version is **1** or **2**.
VlanQuerier	IP address of the IGMP querier.
VlanQueryMaxResponse Time	Maximum query response time (in tenths of a second).
VlanRobustness	Robustness value.
VlanLastMemberQueryIntvl	Last member query interval. This is the maximum response time inserted into group-specific queries which are sent in response to Leave Group messages. It is also the amount of time between group-specific query messages.
VlanQuerierUpTime	Time (in seconds) the IGMP querier has been active.

set igmp config

Use this command to configure IGMP settings on one or more VLANs.

Syntax

set igmp config *vlan-list* {[**query-interval** *query-interval*] [**igmp-version** *igmp-version*] [**max-resp-time** *max-resp-time*] [**robustness** *robustness*] [**last-mem-int** *last-mem-int*]}

Parameters

vlan-list	Specifies the VLAN(s) on which to configure IGMP.
query-interval *query-interval*	(Optional) Specifies the frequency of host-query frame transmissions. Valid values are from **1** to **65535** seconds. This value works together with *max-resp-time* to remove ports from an IGMP group.
igmp-version *igmp-version*	(Optional) Specifies the IGMP version. Valid values are: • **1 -** IGMP V1 • **2** - IGMP V2
max-resp-time *max-resp-time*	(Optional) Specifies the maximum query response time. Valid values are **1** to **25** seconds. This value works together with *query-interval* to remove ports from an IGMP group.
robustness *robustness*	(Optional) Specifies the robustness value. This can be increased to tune for expected packet loss on a subnet. Valid values are **2** to **255.**
last-mem-int *last-mem-int*	(Optional) Specifies the Last Member Query Interval. This is the maximum response time inserted into group-specific queries which are sent in response to Leave Group messages. It is also the amount of time between group-specific query messages. Valid values are **1** to **255.**

Defaults

At least one optional parameter must be specified.

Mode

Switch command, Read-Write.

Downloaded from www.Manualslib.com manuals search engine

Example

This example shows how to set the IGMP query interval time to 250 seconds on VLAN 1:

```
Matrix(rw)->set igmp config 1 query-interval 250
```

set igmp delete

Use this command to remove IGMP configuration settings for one or more VLANs.

Syntax

set igmp delete *vlan-list*

Parameters

vlan-list	Specifies the VLAN(s) on which configuration settings will be cleared.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to remove IGMP configuration settings for VLAN 104:

```
Matrix(rw)->set igmp delete 104
```

show igmp groups

Use this command to display information about IGMP groups known to one or more VLANs.

Syntax

show igmp groups [**group** *group*] [**vlan-list** *vlan-list*] [**sip** *sip*] [**-verbose**]

Parameters

group	Group IP address (Entering no IP address shows all groups).
vlan-list	Specifies the VLAN(s) for which to display IGMP group information.
sip	Source IP address (Entering no sip shows all sips).
-verbose	Show verbose display.

Defaults

None.

Mode

Switch command, Read-Only.

Downloaded from www.Manualslib.com manuals search engine

Example

This example shows how to display IGMP group information for VLAN 105. In this example, the device knows to forward all multicast traffic for IP group address 224.0.0.2 (VLAN 105) to Fast Ethernet port 2 in module 2, and 1-Gigabit Ethernet port 14 in module 3:

```
Matrix(rw)->show igmp groups 105
------------------------------------------------------------
Vlan Id       = 105 Multicast Group Address = 224.0.0.2    Type = IGMP
IGMP Port List = fe.2.2 ge.3.14
```

show igmp static

Use this command to display static IGMP ports for one or more VLANs or IGMP groups.

Syntax

show igmp static *vlan-list* [**group** *group*]

Parameters

vlan-list	Specifies the VLAN(s) for which to display static IGMP information.
group *group*	(Optional) Displays information for a specific IGMP group (IP address).

Defaults

If not specified, static IGMP information will be displayed for all groups.

Mode

Switch command, Read-Only.

Example

This example shows how to display static IGMP information for VLAN 105. The display is similar to the **show igmp groups** display:

```
Matrix(rw)->show igmp static 105
------------------------------------------------------------
Vlan Id       = 105 Multicast Group Address = 224.0.0.2    Type = IGMP
IGMP Port List = fe.2.2 ge.3.14
```

set igmp add-static

Use this command to create a new static IGMP entry, or to add one or more new ports to an existing entry.

Syntax

set igmp add-static *group vlan-list* [**modify**] [**include-ports**] [**exclude-ports**]

Parameters

group	Specifies a group IP address for the entry.
vlan-list	Specifies the VLAN(s) on which to configure the entry.

Downloaded from www.Manualslib.com manuals search engine

modify	(Optional) Adds new ports to an existing entry.
include-ports	(Optional) Port or range of ports.
exclude-ports	(Optional) Port or range of ports.

Defaults

If not specified, the static entry will be created and not modified.

Mode

Switch command, Read-Write.

Example

This example shows how to add port fe.1.3 to the IGMP group at 224.0.2 (VLAN 105):

```
Matrix(rw)->set igmp add-static 224.0.0.2 105 modify include-ports fe.1.3
```

set igmp remove-static

Use this command to delete a static IGMP entry, or to remove one or more ports from an existing entry.

Syntax

set igmp remove-static *group vlan-list* [**modify**] [**include-ports**] [**exclude-ports**]

Parameters

group	Specifies a group IP address for the entry.
vlan-list	Specifies the VLAN(s) on which to configure the entry.
modify	(Optional) Adds new ports to an existing entry.
include-ports	(Optional) Port or range of ports.
exclude-ports	(Optional) Port or range of ports.

Defaults

If not specified, the static entry will be removed and not modified.

Mode

Switch command, Read-Write.

Example

This example shows how to remove port fe.1.3 from the IGMP group at 224.0.2 (VLAN 105):

```
Matrix(rw)->set igmp remove-static 224.0.0.2 105 modify include-ports fe.1.3
```


Downloaded from www.Manualslib.com manuals search engine

show igmp protocols

Use this command to display the binding of IP protocol id to IGMP classification.

Syntax

show igmp protocols

Defaults

None.

Mode

Switch command, Read-Only.

Example

This example shows how to display the binding of IP protocol id to IGMP classification:

```
Matrix(rw)->show igmp protocols
Protocol Classifications

Protocol Ids set to Mcast Data
17

Protocol Ids set to routing Protocol
3,7-9,42-43,45,47-48,85-86,88-89,91-92,100,103,112

Protocol Ids set to Ignore
0,4-6,10-16,18-41,44,46,49-84,87,90,93-99,101-102,104-111,113-255
```

set igmp protocols

Use this command to changes the IGMP classification of received IP frames

Syntax

set igmp protocols [**classification** *classification*] [**protocol-id** *protocol-id*] [**modify**]

Parameters

classification *classification*	Specifies the classification. Options are: • **1**-multicast data • **2**-routing protocol • **3**-ignore
protocol-id *protocol-id*	The protocol ids to change(0-255).
modify	Add to existing classifications. If not used, protocols will be overwritten.

Downloaded from www.Manualslib.com manuals search engine

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to change IGMP routing protocols to a protocol id of 3:

```
Matrix(rw)->set igmp protocols classification 2 protocol-id 3 modify
```

clear igmp protocols

Use this command to clear the binding of IP protocol id to IGMP classification

Syntax

clear igmp protocols [**protocol-id** *protocol-id*]

Parameters

protocol-id *protocol-id*	The protocol ids to change (0-255).

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to clear IGMP protocols for protocol id 3:

```
Matrix(rw)->clear igmp protocols protocol-id 3
```

show igmp vlan

Use this command to display IGMP information for a specific VLAN.

Syntax

show igmp vlan [*vlan-list*]

Parameters

vlan-list	(Optional) Show IGMP info for the given VLAN.

Defaults

If *vlan-list* is not displayed, information for all VLANs are displayed.

Mode

Switch command, Read-Only.

Downloaded from www.Manualslib.com manuals search engine

Example

This example shows how to display igmp information for vlan 12:

```
Matrix(rw)->show igmp vlan 12
IGMP Vlan 12 Info
IGMP query state            : Enabled
QueryInterval(sec.)         : 125
Status                      : Active
IGMP Version                : 2
Querier                     : 2.25.0.1
QueryMaxResponseTime(sec.)  : 10
Robustness                  : 2
LastMemberQueryIntvl(sec.)  : 10
QuerierUpTime               : 4 D  23 H  8 M
Router(s) on ports          : none.
Egressing ports             : lag.0.1-2,4
```

show igmp reporters

Use this command to display IGMP reporter information.

Syntax

show igmp reporters [**portlist** *portlist*] [**group** *group*] [**vlan-list** *vlan-list*] [**sip** *sip*]

Parameters

portlist *portlist*	(Optional) Port or range of ports.
group *group*	(Optional) Group IP address (none means show all groups)
vlan-list *vlan-list*	(Optional) VLAN ID or range of IDs (1-4094)
sip *sip*	(Optional) Source IP address (none means show all sips)

Defaults

If no parameters are specified, all IGMP reporter information is displayed.

Mode

Switch command, Read-Only.

Example

This example shows how to display the all IGMP reporter information :

```
Matrix(rw)->show igmp reporters
IGMP Reporters

 Port    Group Address  Vlan Source IP ExpireTime(Sec) Flags
 ---------------------------------------------------------------
 lag.0.2  224.0.0.251     1   Any     252             DYNAMIC
```


Downloaded from www.Manualslib.com manuals search engine

```
lag.0.2  239.255.12.43   1   Any     253             DYNAMIC
lag.0.2  239.255.255.250 1   Any     255             DYNAMIC
lag.0.2  239.255.255.250 20  Any     249             DYNAMIC
lag.0.4  235.80.68.83    20  Any     237             DYNAMIC
lag.0.4  239.255.255.250 20  Any     243             DYNAMIC
```

show igmp flows

Use this command to display IGMP flow information.

Syntax

show igmp flows [**portlist** *portlist*] [**group** *group*] [**vlan-list** *vlan-list*] [**sip** *sip*]

Parameters

portlist *portlist*	(Optional) Port or range of ports.
group *group*	(Optional) Group IP address (none means show all groups)
vlan-list *vlan-list*	(Optional) VLAN ID or range of IDs (1-4094)
sip *sip*	(Optional) Source IP address (none means show all sips)

Defaults

If no parameters are specified, information for all IGMP flows is displayed.

Mode

Switch command, Read-Only.

Example

This example shows how to display all the IGMP flow information:

```
Matrix(rw)->show igmp counters
Multicast Flows

 Src Port   Group Address   Vlan      Src IP
 ---------------------------------------------
 fe.1.20     224.1.1.1       1      45.67.89.23
 fe.1.36     224.1.1.2       1      39.47.23.67
```

show igmp counters

Use this command to display IGMP counter information.

Syntax

show igmp counters

Parameters

None.

Downloaded from www.Manualslib.com manuals search engine

Defaults

None.

Mode

Switch command, Read-Only.

Example

This example shows how to display the IGMP counters:

```
Matrix(rw)->show igmp counters
Igmp Counters:
 Igmp Group Table is Full                 : false
 Igmp Version 1 Queries transmitted       : 0
 Igmp Version 2 Queries transmitted       : 1016368
 Igmp Version 3 Queries transmitted       : 0
 Igmp Group Specific Queries transmitted  : 0
 Igmp Queries received                    : 776482
 Igmp Version 1 Joins received            : 0
 Igmp Version 2 Joins received            : 1024
 Igmp Version 3 Joins received            : 22
 Igmp Leave Groups received               : 0
 Igmp Dropped Frames                      : 22
```

Usage

show igmp number-groups

Use this command to display the number of multicast groups supported by the Enterasys Matrix device.

Syntax

```
show igmp number-groups
```

Parameters

None.

Defaults

None.

Mode

Switch command, Read-write.

Usage

The command displays both the currently active number of groups and the configured number that will take effect at the next reboot.

Downloaded from www.Manualslib.com manuals search engine

Example

This example shows how to display the number of multicast groups supported by the device.

```
Matrix(rw)->show igmp number-groups
IGMP current max number of groups = 4096
IGMP stored max number of groups = 4096
```


Downloaded from www.Manualslib.com manuals search engine

10

System Logging Configuration

This chapter describes system logging commands and how to use them.

Note: An Enterasys Feature Guide document that contains a complete discussion on Syslog configuration exists at the following Enterasys web site: http://www.enterasys.com/support/manuals/

Configuring System Logging

Purpose

To display and configure system logging, including Syslog server settings, logging severity levels for various applications, Syslog default settings, and the logging buffer.

Commands

For information about...	Refer to page...
show logging all	10-2
show logging server	10-3
set logging server	10-4
clear logging server	10-5
show logging default	10-5
set logging default	10-6
clear logging default	10-7
show logging application	10-7
set logging application	10-9
clear logging application	10-11
show logging local	10-11
set logging local	10-12
clear logging local	10-12
set logging here	10-13
clear logging here	10-13
show logging buffer	10-14

Downloaded from www.Manualslib.com manuals search engine

show logging all

Use this command to display all configuration information for system logging.

Syntax

show logging all

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Only.

Example

This example shows how to display all system logging information:

```
Matrix(rw)->show logging all
        Application   Current Severity Level Server List
-------------------------------------------------------------
 88     RtrAcl                    6              1-8
 89     CLI                       6              1-8
 90     SNMP                      6              1-8
 91     Webview                   6              1-8
 93     System                    6              1-8
 95     RtrFe                     6              1-8
 96     Trace                     6              1-8
 105    RtrLSNat                  6              1-8
 111    FlowLimt                  6              1-8
 112    UPN                       6              1-8
 117    AAA                       6              1-8
 118    Router                    6              1-8
 140    AddrNtfy                  6              1-8
 141    OSPF                      6              1-8
 142    VRRP                      6              1-8
 145    RtrArpProc                6              1-8
 147    LACP                      6              1-8

1(emergencies)  2(alerts)       3(critical)
4(errors)       5(warnings)     6(notifications)
7(information)  8(debugging)

  IP Address       Facility Severity        Description       Port Status
-------------------------------------------------------------------------
```


Downloaded from www.Manualslib.com manuals search engine

```
 1 80.80.80.252    local7 debugging(8)      N-Series           514 enabled


Defaults:          local4 debugging(8)                         514


Syslog Console Logging enabled

Syslog File Logging disabled
```

Table 10-1 provides an explanation of the command output.

Table 10-1 show logging all Output Details

Output...	What it displays...
Application	A mnemonic abbreviation of the textual description for applications being logged.
Current Severity Level	Severity level (**1** - **8**) at which the server is logging messages for the listed application. For details on setting this value using the **set logging application** command, refer to "set logging application" on page 10-9.
Defaults	Default facility name, severity level and UDP port designation (as described below.) For details on setting this value using the **set logging defaults** command, refer to "set logging default" on page 10-6.
IP Address	Syslog server's IP address. For details on setting this using the **set logging server** command, refer to "set logging server" on page 10-4.
Facility	Syslog facility that will be encoded in messages sent to this server. Valid values are: **local0** to **local7**.
Severity	Severity level at which the server is logging messages.
Description	Text string description of this facility/server.
Port	UDP port the client uses to send to the server.
Status	Whether or not this Syslog configuration is currently enabled or disabled.

show logging server

Use this command to display the Syslog configuration for a particular server.

Syntax

show logging server [*index*]

Parameters

index	(Optional) Displays Syslog information pertaining to a specific server table entry. Valid values are **1**-**8**.

Downloaded from www.Manualslib.com manuals search engine

Defaults

If *index* is not specified, all Syslog server information will be displayed.

Mode

Switch command, Read-Only.

Example

This example shows how to display Syslog server configuration information. For an explanation of the command output, refer back to Table 10-1.

```
Matrix(rw)->show logging server

IP Address       Facility Severity        Description       Port Status
-------------------------------------------------------------------------
 1 132.140.82.111 local4 warning(5)        default         514 enabled
 2 132.140.90.84  local4 warning(5)        default         514 enabled
```

set logging server

Use this command to configure a Syslog server.

Syntax

set logging server *index* [**ip-addr** *ip-addr*] [**facility** *facility*] [**severity** *severity*] [**descr** *descr*] [**port** *port*] [**state** {**enable** | **disable**}]

Parameters

index	Specifies the server table index number for this server. Valid values are **1** - **8**.
ip-addr *ip-addr*	(Optional) Specifies the Syslog message server's IP address.
facility *facility*	(Optional) Specifies the server's facility name. Valid values are: **local0** to **local7**.
severity *severity*	(Optional) Specifies the severity level at which the server will log messages. Valid values and corresponding levels are: **1** - emergencies (system is unusable) **2** - alerts (immediate action required) **3** - critical conditions **4** - error conditions **5** - warning conditions **6** - notifications (significant conditions) **7** - informational messages **8** - debugging messages
descr *descr*	(Optional) Specifies a textual string description of this facility/server.
port *port*	(Optional) Specifies the default UDP port the client uses to send to the server.
state enable | **disable**	(Optional) Enables or disables this facility/server configuration.

Downloaded from www.Manualslib.com manuals search engine

Defaults

- If **ip-addr** is not specified, an entry in the Syslog server table will be created with the specified *index* number and a message will display indicating that no IP address has been assigned.
- If not specified, **facility**, severity and port will be set to defaults configured with the s**et logging default** command ("set logging default" on page 10-6.).
- If **state** is not specified, the server will not be enabled or disabled.

Mode

Switch command, Read-Write.

Example

This command shows how to enable a Syslog server configuration for index 1, IP address 134.141.89.113, facility local4, severity level 3 on port 514:

```
Matrix(rw)->set logging server 1 ip-addr 134.141.89.113 facility local4 severity
3 port 514 state enable
```

clear logging server

Use this command to remove a server from the Syslog server table.

Syntax

clear logging server *index*

Parameters

index	Specifies the server table index number for the server to be removed. Valid values are **1** - **8**.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This command shows how to remove the Syslog server with index 1 from the server table:

```
Matrix(rw)->clear logging server 1
```

show logging default

Use this command to display the Syslog server default values.

Syntax

show logging default

Parameters

None.

Downloaded from www.Manualslib.com manuals search engine

Defaults

None.

Mode

Switch command, Read-Only.

Example

This command shows how to display the Syslog server default values. For an explanation of the command output, refer back to Table 10-1.

```
Matrix(rw)->show logging default.


              Facility      Severity          Port
           ----------------------------------------
Defaults:     local4       warning(5)       514
```

set logging default

Use this command to set logging default values.

Syntax

set logging default {[**facility** *facility*] [**severity** *severity*] **port** *port*]}

Parameters

facility *facility*	Specifies the default facility name. Valid values are: **local0** to **local7**.
severity *severity*	Specifies the default logging severity level. Valid values and corresponding levels are: **1** - emergencies (system is unusable) **2** - alerts (immediate action required) **3** - critical conditions **4** - error conditions **5** - warning conditions **6** - notifications (significant conditions) **7** - informational messages **8** - debugging messages
port *port*	Specifies the default UDP port the client uses to send to the server.

Defaults

None.

Mode

Switch command, Read-Write.

Downloaded from www.Manualslib.com manuals search engine

Example

This example shows how to set the Syslog default facility name to local2 and the severity level to 4 (error logging):

```
Matrix(rw)->set logging default facility local2 severity 4
```

clear logging default

Use this command to reset logging default values.

Syntax

clear logging default{[**facility**] [**severity**] [**port**]}

Parameters

facility	(Optional) Resets the default facility name to **local4**.
severity	(Optional) Resets the default logging severity level to **6** (notifications of significant conditions).
port	(Optional) Resets the default UDP port the client uses to send to the server to **514**.

Defaults

- At least one optional parameter must be entered.
- All three optional keywords must be entered to reset all logging values to defaults.

Mode

Switch command, Read-Write.

Example

This example shows how to reset the Syslog default severity level to 6:

```
Matrix(rw)->clear logging default severity
```

show logging application

Use this command to display the severity level of Syslog messages for one or all applications configured for logging on your system.

Syntax

show logging application [*mnemonic* | **all**]

Parameters

mnemonic | **all**	(Optional) Displays severity level for one or all applications configured for logging.

Defaults

If not specified, information for all applications will be displayed.

Downloaded from www.Manualslib.com manuals search engine

Mode

Switch command, Read-Only.

Usage

Mnemonics will vary depending on the number and types of applications running on your system. To display a complete list, use the **show logging application** command as described in "show logging application" on page 10-7. Sample values and their corresponding applications are listed in Table 10-3.

Mnemonic values are case sensitive and must be typed as they appear in Table 10-3.

Example

This example shows how to display system logging information pertaining to the all supported applications.

```
Matrix(su)->show logging application

       Application   Current Severity Level Server List
-----------------------------------------------------------
 88     RtrAcl                   6              1-8
 89     CLI                      6              1-8
 90     SNMP                     6              1-8
 91     Webview                  6              1-8
 93     System                   6              1-8
 95     RtrFe                    6              1-8
 96     Trace                    6              1-8
 105    RtrLSNat                 6              1-8
 111    FlowLimt                 6              1-8
 112    UPN                      6              1-8
 117    AAA                      6              1-8
 118    Router                   6              1-8
 140    AddrNtfy                 6              1-8
 141    OSPF                     6              1-8
 142    VRRP                     6              1-8
 145    RtrArpProc               6              1-8
 147    LACP                     6              1-8

1(emergencies)  2(alerts)       3(critical)
4(errors)       5(warnings)     6(notifications)
7(information)  8(debugging)
```

This example shows how to display system logging information pertaining to the SNMP application.

```
Matrix(rw)->show logging application SNMP

        Application   Current Severity Level Server List
-----------------------------------------------------------
```


Downloaded from www.Manualslib.com manuals search engine

```
 90      SNMP                        6               1-8

1(emergencies)   2(alerts)        3(critical)
4(errors)        5(warnings)      6(notifications)
7(information)   8(debugging)
```

Table 10-2 provides an explanation of the command output.

Table 10-2 show logging application Output Details

Output...	What it displays...
Application	A mnemonic abbreviation of the textual description for applications being logged.
Current Severity Level	Severity level at which the server is logging messages for the listed application. This range (from 1 to 8) and its associated severity list is shown in the CLI output. For a description of these entries, which are set using the **set logging application** command, refer to "set logging application" on page 10-9.
Server List	Servers to which log messages are being sent.

set logging application

Use this command to set the severity level of log messages and the server(s) to which messages will be sent for one or all applications.

Syntax

set logging application {[*mnemonic* | **all**]} [**level** *level*] [**servers** *servers*]

Parameters

mnemonic	Specifies a case sensitive mnemonic abbreviation of an application to be logged. This parameter will vary depending on the number and types of applications running on your system. To display a complete list, use the **show logging application** command as described in "show logging application" on page 10-7. Sample values and their corresponding applications are listed in Table 10-3.
all	Sets the logging severity level for all applications.
level *level*	(Optional) Specifies the severity level at which the server will log messages for applications. Valid values and corresponding levels are: **1** - emergencies (system is unusable) **2** - alerts (immediate action required) **3** - critical conditions **4** - error conditions **5** - warning conditions **6** - notifications (significant conditions) **7** - informational messages **8** - debugging messages
servers *servers*	(Optional) Specifies index number(s) of the Syslog server(s) to which messages will be sent. Valid values are **1** - **8** and are set using the **set logging server** command ("set logging server" on page 10-4).

Downloaded from www.Manualslib.com manuals search engine

Defaults

- If **level** is not specified, none will be applied.
- If **server** is not specified, messages will be sent to all Syslog servers.

Mode

Switch command, Read-Write.

Usage

Mnemonic values are case sensitive and must be typed as they appear in Table 10-3.

Table 10-3 Sample Mnemonic Values for Logging Applications

Mnemonic	Application
AAA	Authentication, Authorization, & Accounting
AddrNtfy	Address Add and Move Notification
CLI	Command Line Interface
FlowLimit	Flow Limiting
LACP	Link Aggregation Control Protocol
OSPF	Open Shortest Path First Routing Protocol
Router	Router
RtrAcl	Router Access Control List
RtrFE	Router Forwarding Engine
RtrArpProc	Router Arp Process
RtrLSNat	Router Load Sharing Network Address Translation
SNMP	Simple Network Management Protocol
System	Non-Application items such as general blade/chassis/ configurations, etc.
Trace	Router Tracing
UPN	User Personalized Networking
VRRP	Virtual Router Redundancy Protocol
Webview	Webview Device Management

Example

This example shows how to set the severity level for SSH (Secure Shell) to 4 so that error conditions will be logged for that application and sent to Syslog server 1:

```
Matrix(rw)->set logging application SSH level 4 server 1
```


Downloaded from www.Manualslib.com manuals search engine

clear logging application

Use this command to reset the logging severity level for one or all applications to the default value of 6 (notifications of significant conditions).

Syntax

clear logging application {*mnemonic* | **all**}

Parameters

mnemonic | **all**	(Optional) Resets the severity level for a specific application or for all applications. Valid mnemonic values and their corresponding applications are listed in Table 10-3.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to reset the logging severity level for SSH:

```
Matrix(rw)->clear logging application SSH
```

show logging local

Use this command to display the state of message logging to the console and a persistent file.

Syntax

show logging local

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Only.

Example

This example shows how to display the state of message logging. In this case, logging to the console is enabled and logging to a persistent file is disabled.

```
Matrix(rw)->show logging local
Syslog Console Logging enabled
Syslog File Logging disabled
```


Downloaded from www.Manualslib.com manuals search engine

set logging local

Use this command to configure log messages to the console and a persistent file.

Syntax

```
set logging local console {enable | disable} file {enable | disable}
```

Parameters

console enable | **disable**	Enables or disables logging to the console.
file enable | **disable**	Enables or disables logging to a persistent file.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This command shows how to enable logging to the console and disable logging to a persistent file:

```
Matrix(rw)->set logging local console enable file disable
```

clear logging local

Use this command to clear the console and persistent store logging for the local session.

Syntax

```
clear logging local
```

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to clear local logging:

```
Matrix(rw)->clear logging local
```


Downloaded from www.Manualslib.com manuals search engine

set logging here

Use this command to enable or disable the current CLI session as a Syslog destination.

Syntax

set logging here {**enable** | **disable**}

Parameters

enable | **disable**	Enables or disables display of logging messages for the current CLI session.

Defaults

None.

Mode

Switch command, Read-Write.

Usage

The effect of this command will be temporary if the current CLI session is using Telnet or SSH, but persistent on the console.

Example

This command shows how to enable the display of logging messages to the current CLI session:

```
Matrix(rw)->set logging here enable
```

clear logging here

Use this command to clear the logging state for the current CLI session.

Syntax

clear logging here

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This command shows how to clear the logging state for the current CLI session:

```
Matrix(rw)->clear logging here
```


Downloaded from www.Manualslib.com manuals search engine

show logging buffer

Use this command to display the last 256 messages logged on all blades.

Syntax

```
show logging buffer
```

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Only.

Example

This example shows a portion of the information displayed with the **show logging buffer** command

```
Matrix(rw)->show logging buffer
<165>Sep  4 07:43:09 10.42.71.13 CLI[5]User:rw logged in from 10.2.1.122 (telnet)
<165>Sep  4 07:43:24 10.42.71.13 CLI[5]User: debug failed login from 10.4.1.100
(telnet)
```


Downloaded from www.Manualslib.com manuals search engine

11

Network Monitoring Configuration

This chapter describes Network Monitoring commands and how to use them.

For information about...	Refer to page...
Monitoring Network Events and Status	11-1
Configuring SMON	11-8
Configuring RMON	11-13

Monitoring Network Events and Status

Purpose

To display switch events and command history, to set the size of the history buffer, and to display and disconnect current user sessions.

Commands

For information about...	Refer to page...
history	11-1
show history	11-2
set history	11-3
show netstat	11-3
ping	11-4
show users	11-6
tell	11-6
disconnect	11-7

history

Use this command to display the contents of the command history buffer.

Syntax

```
history
```


Downloaded from www.Manualslib.com manuals search engine

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Only.

Usage

The command history buffer includes all the switch commands entered up to a maximum of 50, as specified in the **set history** command ("set history" on page 11-3).

Example

This example shows how to display the contents of the command history buffer. It shows there are five commands in the buffer:

```
Matrix(rw)->history
 1 hist
 2 show gvrp
 3 show vlan
 4 show igmp
 5 show ip address
```

show history

Use this command to display the size (in lines) of the history buffer.

Syntax

show history

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Only.

Example

This example shows how to display the size of the history buffer:

```
Matrix(rw)->show history
 History buffer size: 20
```


Downloaded from www.Manualslib.com manuals search engine

set history

Use this command to set the size of the history buffer.

Syntax

set history *size* [**default**]

Parameters

size	Specifies the size of the history buffer in lines. Valid values are **1** to **100**.
default	(Optional) Makes this setting persist for all future sessions.

Defaults

If **default** is not specified, the history setting will not be persistent.

Mode

Switch command, Read-Write.

Example

This example shows how to set the size of the command history buffer to 3 lines and make this the default setting:

```
Matrix(rw)->set history 3 default
```

show netstat

Use this command to display statistics for the switch's active network connections.

Syntax

show netstat [**icmp** | **ip** | **routes** | **stats** | **tcp** | **udp**]

Parameters

icmp	(Optional) Shows Internet Control Message Protocol (ICMP) statistics.
ip	(Optional) Shows Internet Protocol (IP) statistics.
routes	(Optional) Shows the IP routing table.
stats	(Optional) Shows all statistics for TCP, UDP, IP, and ICMP.
tcp	(Optional) Shows Transmission Control Protocol (TCP) statistics.
udp	(Optional) Shows User Datagram Protocol (UDP) statistics.

Defaults

If no parameters are specified, **show netstat** will be executed as shown in the example below.

Mode

Switch command, Read-Only.

Downloaded from www.Manualslib.com manuals search engine

Example

This example shows how to display statistics for all the current active network connections:

```
Matrix(rw)->show netstat
Active Internet connections (including servers)
PCB      Proto Recv-Q Send-Q  Local Address      Foreign Address    (state)
-------- ----- ------ ------  ------------------ ------------------ -------
1cc6314  TCP        0      0  0.0.0.0.80         0.0.0.0.0          LISTEN
1cc6104  TCP        0      0  0.0.0.0.23         0.0.0.0.0          LISTEN
1cc6290  UDP        0      0  0.0.0.0.162        0.0.0.0.0
1cc620c  UDP        0      0  0.0.0.0.161        0.0.0.0.0
```

Table 11-1 provides an explanation of the command output.

Table 11-1 show netstat Output Details

Output...	What it displays...
PCB	Protocol Control Block designation.
Proto	Type of protocol running on the connection.
Recv-Q	Number of queries received over the connection.
Send-Q	Number of queries sent over the connection.
Local Address	IP address of the connection's local host.
Foreign Address	IP address of the connection's foreign host.
(state)	Communications mode of the connection (listening, learning or forwarding).

ping

Use this command to send ICMP echo-request packets to another node on the network from the switch CLI.

Syntax

ping [**-s**] *host* [*count*]

Parameters

-s	(Optional) Causes a continuous ping, sending one datagram per second and printing one line of output for every response received, until the user enters Ctrl+C.
host	Specifies the IP address of the device to which the **ping** will be sent.
count	(Optional) Specifies the number of packets to send. Valid values are from **1** to **2147483647**.

Defaults

- If **-s** is not specified, the ping will not be continuous.
- If not specified, packet *count* will be 1.

Downloaded from www.Manualslib.com manuals search engine

Mode

Switch command, Read-Write.

Examples

Matrix(rw)->ping 134.141.89.29This example shows how to ping IP address 134.141.89.29. In this case, this host is alive:

```
134.141.89.29 is alive
```

Matrix(rw)->ping 134.141.89.255In this example, the host at IP address is not responding:

```
no answer from 134.141.89.255
```

This example shows how to ping IP address 134.141.89.29 with 10 packets:

```
Matrix(rw)->ping 134.141.89.29 10
PING 134.141.89.29: 56 data bytes
64 bytes from 134.141.89.29: icmp-seq=0. time=0. ms
64 bytes from 134.141.89.29: icmp-seq=1. time=0. ms
64 bytes from 134.141.89.29: icmp-seq=2. time=0. ms
64 bytes from 134.141.89.29: icmp-seq=3. time=0. ms
64 bytes from 134.141.89.29: icmp-seq=4. time=0. ms
64 bytes from 134.141.89.29: icmp-seq=5. time=0. ms
64 bytes from 134.141.89.29: icmp-seq=6. time=0. ms
64 bytes from 134.141.89.29: icmp-seq=7. time=0. ms
64 bytes from 134.141.89.29: icmp-seq=8. time=0. ms
64 bytes from 134.141.89.29: icmp-seq=9. time=0. ms ----134.141.89.29 PING
Statistics---- 10 packets transmitted, 10 packets received, 0% packet loss round-
trip (ms)  min/avg/max = 0/0/0
```

This example shows a continuous ping of IP address 134.141.89.29. In this case, entering Ctrl+C after 9 iterations caused command execution to stop:

```
Matrix(rw)->ping -s 134.141.89.29
PING 134.141.89.29: 56 data bytes
64 bytes from 134.141.89.29: icmp-seq=0. time=0. ms
64 bytes from 134.141.89.29: icmp-seq=1. time=0. ms
64 bytes from 134.141.89.29: icmp-seq=2. time=0. ms
64 bytes from 134.141.89.29: icmp-seq=3. time=0. ms
64 bytes from 134.141.89.29: icmp-seq=4. time=0. ms
64 bytes from 134.141.89.29: icmp-seq=5. time=0. ms
64 bytes from 134.141.89.29: icmp-seq=6. time=0. ms
64 bytes from 134.141.89.29: icmp-seq=7. time=0. ms
64 bytes from 134.141.89.29: icmp-seq=8. time=0. ms ----134.141.89.29 PING
Statistics---- 9 packets transmitted, 9 packets received, 0% packet loss round-
trip (ms)  min/avg/max = 0/0/0
```


Downloaded from www.Manualslib.com manuals search engine

show users

Use this command to display information about the active console port or Telnet session(s) logged in to the switch.

Syntax

show users

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Only.

Example

This example shows how to use the **show users** command. In this output, there are two Telnet users logged in with Read-Write access privileges from IP addresses 134.141.192.119 and 134.141.192.18:

```
Matrix(rw)->show users
  Session  User  Location
  -------- ----- --------------------------
* telnet   rw    134.141.192.119
  telnet   rw    134.141.192.18
```

tell

Use this command to send a message to one or all users.

Syntax

tell {*dest* | **all**} *message*

Parameters

dest	Specifies the user to which this message will be sent. Valid syntax is user@location.
all	Sends a broadcast message to all users.
message	Text message.

Defaults

None.

Mode

Switch command, Read-Write.

Downloaded from www.Manualslib.com manuals search engine

Example

This example shows how to tell all users about a system reset:

```
Matrix(rw)->tell all system reset scheduled for 1 p.m. today
```

disconnect

Use this command to close an active console port or Telnet session from the switch CLI.

Syntax

disconnect {*ip-addr* | **console**}

Parameters

ip-addr	Specifies the IP address of the Telnet session to be disconnected. This address is displayed in the output shown in "show users" on page 11-6.
console	Closes an active console port.

Defaults

None.

Mode

Switch command, Read-Write.

Examples

This example shows how to close a Telnet session to host 134.141.192.119:

```
Matrix(rw)->disconnect 134.141.192.119
```

This example shows how to close the current console session:

```
Matrix(rw)->disconnect console
```


Downloaded from www.Manualslib.com manuals search engine

Configuring SMON

Purpose

To configure SMON (Switched Network Monitoring) on the device.

Commands

For information about...	Refer to page...
show smon priority	11-8
set smon priority	11-9
clear smon priority	11-9
show smon vlan	11-10
set smon vlan	11-11
clear smon vlan	11-11

show smon priority

Use this command to display SMON user priority statistics. SMON generates aggregated statistics for IEEE 802.1Q VLAN environments.

Syntax

show smon priority [*port-string*] [**priority** *priority*]

Parameters

port-string	(Optional) Displays SMON priority statistics being collected by specific port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.
priority *priority*	(Optional) Displays SMON statistics based on encoded user priority, Valid values are **0** - **7**.

Defaults

- If *port-string* is not specified, SMON statistics for all ports will be displayed.
- If *priority* is not specified, statistics for all priority queues will be displayed.

Mode

Switch command, Read-Only.

Example

This example shows how to display SMON priority 0 statistics for 1-Gigabit Ethernet port 14 in module 3:

```
Matrix(rw)->show smon priority ge.3.14 0
Show Priority Statistics
```


Downloaded from www.Manualslib.com manuals search engine

```
------------------------
Interface = ge.3.14
Owner     = none
Creation  = 0 days 0 hours 6 minutes 39 seconds
Status    = enabled
--------------------

Priority 0 Packets              Octets
----------
Total      7981308              2332402460
Overflow   0                    0
```

set smon priority

Use this command to create, start, or stop priority-encoded SMON user statistics counting.

Syntax

set smon priority {**create** | **enable** | **disable**} *port-string* [*owner*]

Parameters

create | **enable** | **disable**	Creates, enables, or disables SMON priority statistics counting. Create automatically enables (starts) counters.
port-string	Specifies one or more source ports on which to collect statistics. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.
owner	(Optional) Specifies an administratively assigned name of the owner of this entity.

Defaults

If *owner* is not specified, none will be applied.

Mode

Switch command, Read-Write.

Example

This example shows how set the device to gather SMON priority statistics from 1-Gigabit Ethernet port 14 in module 3:

```
Matrix(rw)->set smon priority ge.3.14
```

clear smon priority

Clears priority-encoded user statistics on one or more ports.

Syntax

clear smon priority [*port-string*]

Downloaded from www.Manualslib.com manuals search engine

Parameters

port-string	(Optional) Clears statistics for specific port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.

Defaults

If *port-string* is not specified, priority statistics will be cleared on all ports.

Mode

Switch command, Read-Write.

Example

This example shows how clear SMON priority statistics on 1-Gigabit Ethernet source port 14 in module 3:

```
Matrix(rw)->clear smon priority ge.3.14
```

show smon vlan

Use this command to display SMON (Switched Network Monitoring) VLAN statistics.

Syntax

show smon vlan [*port-string*] [**vlan** *vlan-id*]

Parameters

port-string	(Optional) Displays SMON VLAN statistics being collected by specific port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.
vlan *vlan-id*	(Optional) Displays SMON statistics associated with a specific VLAN.

Defaults

- If *port-string* is not specified, SMON statistics for all ports will be displayed.
- If *vlan-id* is not specified, statistics for all VLANs will be displayed.

Mode

Switch command, Read-Only.

Example

This example shows how to display SMON VLAN 1 statistics for 1-Gigabit Ethernet port 14 in module 3:

```
Matrix(rw)->show smon vlan ge.3.14 vlan 1
Show VLAN Statistics
--------------------
Interface = ge.3.14
Owner     = none
Creation  = 0 days 16 hours 4 minutes 34 seconds
```


Downloaded from www.Manualslib.com manuals search engine

```
Status    = enabled
--------------------

VLAN 1                Packets               Octets
Total                 8011072               2070785503
Overflow              0                     0
NonUnicast            0                     0
NonUnicast Overflow   0                     0
```

set smon vlan

Use this command to create, start, or stop SNMP VLAN-related statistics counting.

Syntax

set smon vlan {**create** | **enable** | **disable**} *port-string* [*owner*]

Parameters

create | **enable** | **disable**	Creates, enables, or disables SMON VLAN statistics counting. Create automatically enables (starts) counters.
port-string	Specifies one or more source ports on which to collect statistics. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.
owner	(Optional) Specifies an administratively assigned name of the owner of this entity.

Defaults

If *owner* is not specified, none will be applied.

Mode

Switch command, Read-Write.

Example

This example shows how set the device to gather SMON VLAN-related statistics from 1-Gigabit Ethernet port 14 in module 3:

```
Matrix(rw)->set smon vlan ge.3.14
```

clear smon vlan

Use this command to delete an SMON VLAN statistics counting configuration.

Syntax

```
clear smon vlan [port-string]
```


Downloaded from www.Manualslib.com manuals search engine

Parameters

port-string	(Optional) Clears statistics counting configuration(s) for specific port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.

Defaults

If *port-string* is not specified, VLAN statistics counting configurations will be cleared for all ports.

Mode

Switch command, Read-Write.

Example

This example shows how clear an SMON VLAN statistics counting configuration from 1-Gigabit Ethernet source port 14 in module 3:

```
Matrix(rw)->clear smon vlan ge.3.14
```


Downloaded from www.Manualslib.com manuals search engine

Configuring RMON

RMON Monitoring Group Functions and Commands

RMON (Remote Network Monitoring) provides comprehensive network fault diagnosis, planning, and performance tuning information and allows for interoperability between SNMP management stations and monitoring agents. RMON extends the SNMP MIB capability by defining additional MIBs that generate a much richer set of data about network usage. These MIB "groups" each gather specific sets of data to meet common network monitoring requirements.

Table 11-2 lists the RMON monitoring groups supported on Enterasys Matrix Series devices, each group's function and the elements it monitors, and the associated configuration commands needed.

Table 11-2 RMON Monitoring Group Functions and Commands

RMON Group	What It Does...	What It Monitors...	CLI Command(s)
Statistics	Records statistics measured by the RMON probe for each monitored interface on the device.	Packets dropped, packets sent, bytes sent (octets), broadcast and multicast packets, CRC errors, oversized and undersized packets, fragments, jabbers, and counters for packets.	show rmon stats ("show rmon stats" on page 11-15) set rmon stats ("set rmon stats" on page 11-17) clear rmon stats ("clear rmon stats" on page 11-17)
History	Records periodic statistical samples from a network.	Sample period, number of samples and item(s) sampled.	show rmon history ("show rmon history" on page 11-18) set rmon history ("set rmon history" on page 11-19) clear rmon history ("clear rmon history" on page 11-19)
Alarm	Periodically gathers statistical samples from variables in the probe and compares them with previously configured thresholds. If the monitored variable crosses a threshold, an event is generated.	Alarm type, interval, starting threshold, stop threshold.	show rmon alarm ("show rmon alarm" on page 11-20) set rmon alarm properties ("set rmon alarm properties" on page 11-21) set rmon alarm status ("set rmon alarm status" on page 11-22) clear rmon alarm ("clear rmon alarm" on page 11-23)
Event	Controls the generation and notification of events from the device.	Event type, description, last time event was sent.	show rmon event ("show rmon event" on page 11-24) set rmon event properties ("set rmon event properties" on page 11-25) set rmon event status ("set rmon event status" on page 11-25) clear rmon event ("clear rmon event" on page 11-26)

Downloaded from www.Manualslib.com manuals search engine

Table 11-2 RMON Monitoring Group Functions and Commands (continued)

RMON Group	What It Does...	What It Monitors...	CLI Command(s)
Host	Records statistics associated with each host discovered on the network.	Host address, packets and bytes received and transmitted, and broadcast, multicast and error packets.	show rmon host (“show rmon host” on page 11-27) set rmon host properties (“set rmon host properties” on page 11-28) set rmon host status (“set rmon host status” on page 11-28) clear rmon host (“clear rmon host” on page 11-29)
Host TopN	Generates tables that describe hosts that top a list ordered by one of their statistics. These rate based statistics are samples of one of their base statistics over an interval specified by the management station.	Statistics, top host(s), sample stop and start period, rate base and duration.	show rmon topN (“show rmon topN” on page 11-29) set rmon topN properties (“set rmon topN properties” on page 11-31) set rmon topN status (“set rmon topN status” on page 11-31) clear rmon topN (“clear rmon topN” on page 11-32)
Matrix	Records statistics for conversations between two IP addresses. As the device detects a new conversation, it creates a new matrix entry.	Source and destination address pairs and packets, bytes and errors for each pair.	show rmon matrix (“show rmon matrix” on page 11-32) set rmon matrix properties (“set rmon matrix properties” on page 11-34) set rmon matrix status (“set rmon matrix status” on page 11-34) clear rmon matrix (“clear rmon matrix” on page 11-35)
Filter	Allows packets to be matched by a filter equation. These matched packets form a data stream or “channel” that may be captured or may generate events.	Packets matching the filter configuration.	show rmon channel (“show rmon channel” on page 11-35) set rmon channel (“set rmon channel” on page 11-36) clear rmon channel (“clear rmon channel” on page 11-37) show rmon filter (“show rmon filter” on page 11-37) set rmon filter (“set rmon filter” on page 11-38) clear rmon filter (“clear rmon filter” on page 11-39)
Packet Capture	Allows packets to be captured upon a filter match.	Packets matching the filter configuration.	show rmon capture (“show rmon capture” on page 11-40) set rmon capture (“set rmon capture” on page 11-41) clear rmon capture (“clear rmon capture” on page 11-42)

Downloaded from www.Manualslib.com manuals search engine

show rmon stats

Use this command to display RMON statistics measured for one or more ports.

Syntax

show rmon stats [*port-string*] [**wide**] [**bysize**]

Parameters

port-string	(Optional) Displays RMON statistics for specific port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.
wide	(Optional) Display most important stats, one line per entry.
bysize	(Optional) Display counters by packet length.

Defaults

If *port-string* is not specified, RMON stats will be displayed for all ports.

Mode

Switch command, Read-Only.

Example

This example shows how to display RMON statistics for Fast Ethernet port 20 in module 1:

```
Matrix(rw)->show rmon stats fe.1.20

Port: fe.1.20
--------------------
Index          = 1011
Owner          = monitor
Data Source    = 1.3.6.1.2.1.2.2.1.1.51021

Drop Events    = 0             Packets            = 0
Collisions     = 0             Octets             = 0
Jabbers        = 0             0    -   64 Octets = 0
Broadcast Pkts = 0             65   -  127 Octets = 0
Multicast Pkts = 0             128  -  255 Octets = 0
CRC Errors     = 0             256  -  511 Octets = 0
Undersize Pkts = 0             512  - 1023 Octets = 0
Oversize Pkts  = 0             1024 - 1518 Octets = 0
Fragments      = 0
```

Table 11-3 provides an explanation of the command output.

Downloaded from www.Manualslib.com manuals search engine

Table 11-3 show rmon stats Output Details

Output...	What it displays...
Port	Port designation.
Owner	Name of the entity that configured this entry. Monitor is default.
Data Source	Data source of the statistics being displayed.
Drop Events	Total number of times that the switch was forced to discard frames due to lack of available switch device resources. This does not display the number of frames dropped, only the number of times the switch was forced to discard frames.
Collisions	Total number of collisions that have occurred on this interface.
Jabbers	Total number of frames that were greater than 1518 bytes and had either a bad FCS or a bad CRC.
Packets	Total number of frames (including bad frames, broadcast frames, and multicast frames) received on this interface.
Broadcast Pkts	Total number of good frames that were directed to the broadcast address. This value does not include multicast frames.
Multicast Pkts	Total number of good frames that were directed to the multicast address. This value does not include broadcast frames.
CRC Errors	Number of frames with bad Cyclic Redundancy Checks (CRC) received from the network. The CRC is a 4-byte field in the data frame that ensures that the data received is the same as the data that was originally sent.
Undersize Pkts	Number of frames received containing less than the minimum Ethernet frame size of 64 bytes (not including the preamble) but having a valid CRC.
Oversize Pkts	Number of frames received that exceeded 1518 data bytes (not including the preamble) but had a valid CRC.
Fragments	Number of received frames that are not the minimum number of bytes in length, or received frames that had a bad or missing Frame Check Sequence (FCS), were less than 64 bytes in length (excluding framing bits, but including FCS bytes) and had an invalid CRC. It is normal for this value to increment since fragments are a normal result of collisions in a half-duplex network.
Packets	Total number of packets, including bad, broadcast and multicast.
Octets	Total number of octets (bytes) of data, including those in bad frames, received on this interface.
0 – 64 Octets	Total number of frames, including bad frames, received that were 64 bytes in length (excluding framing bits, but including FCS bytes).
65 – 127 Octets	Total number of frames, including bad frames, received that were between 65 and 127 bytes in length (excluding framing bits, but including FCS bytes).
128 – 255 Octets	Total number of frames, including bad frames, received that were between 128 and 255 bytes in length (excluding framing bits, but including FCS bytes).
256 – 511 Octets	Total number of frames, including bad frames, received that were between 256 and 511 bytes in length (excluding framing bits, but including FCS bytes).

Downloaded from www.Manualslib.com manuals search engine

Table 11-3 show rmon stats Output Details (continued)

Output...	What it displays...
512 – 1023 Octets	Total number of frames, including bad frames, received that were between 512 and 1023 bytes in length (excluding framing bits, but including FCS bytes).
1024 – 1518 Octets	Total number of frames, including bad frames, received that were between 1024 and 1518 bytes in length (excluding framing bits, but including FCS bytes).

set rmon stats

Use this command to configure an RMON statistics entry.

Syntax

set rmon stats *index port-string* [*owner*]

Parameters

index	Specifies an index for this statistics entry.
port-string	Specifies port(s) to which this entry will be assigned. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.
owner	(Optional) Assigns an owner for this entry.

Defaults

If *owner* is not specified, **monitor** will be applied.

Mode

Switch command, Read-Write.

Example

This example shows how to configure RMON statistics entry 2 for fe.1.20:

```
Matrix(rw)->set rmon stats 2 fe.1.20
```

clear rmon stats

Use this command to delete one or more RMON statistics entries.

Syntax

clear rmon stats {*index-list* | **to-defaults**}

Parameters

index-list	Specifies one or more stats entries to be deleted, causing them to disappear from any future RMON queries.
to-defaults	Resets all history entries to default values. This will cause entries to reappear in RMON queries.

Downloaded from www.Manualslib.com manuals search engine

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to delete RMON statistics entry 2:

```
Matrix(rw)->clear rmon stats 2
```

show rmon history

Use this command to display RMON history properties and statistics. The RMON history group records periodic statistical samples from a network.

Syntax

show rmon history [*port-string*] [**wide**] [**interval**]

Parameters

port-string	(Optional) Displays RMON history entries for specific port(s).
wide	(Optional) Display most important stats, one line per entry.
interval	(Optional) Summarize history over a fixed interval.

Defaults

If *port-string* is not specified, information about all RMON history entries will be displayed.

Mode

Switch command, Read-Only.

Example

This example shows how to display RMON history entries for Fast Ethernet port 14 in module 3. A control entry displays first, followed by actual entries corresponding to the control entry. In this case, the default settings for entry owner, sampling interval, and maximum number of entries. (buckets) have not been changed from their default values (as described in "set rmon history" on page 11-19). For a description of the types of statistics shown, refer to Table 11-3:

```
Matrix(rw)->show rmon history fe.3.14
Port: fe.3.14
---------------------------------------
Index 1001
Status            = 1 valid
Owner             = monitor
Data Source       = 1.3.6.1.2.1.2.2.1.1.11001
Interval          = 30
Buckets Requested = 50
Buckets Granted   = 50
```


Downloaded from www.Manualslib.com manuals search engine

```
Sample 2304      Interval Start: 0 days 19 hours 11 minutes 35 seconds
Drop Events       = 0                    Undersize Pkts    = 0
Octets            = 0                    Oversize Pkts     = 0
Packets           = 0                    Fragments         = 0
Broadcast Pkts    = 0                    Jabbers           = 0
Multicast Pkts    = 0                    Collisions        = 0
CRC Align Errors  = 0                    Utilization(%)    = 0
```

set rmon history

Use this command to configure an RMON history entry.

Syntax

set rmon history *index* [*port-string*] [**buckets** *buckets*] [**interval** *interval*] [**owner** *owner*]

Parameters

index	Specifies an index number for this entry.
port-string	(Optional) Assigns this entry to a specific port.
buckets *buckets*	(Optional) Specifies the maximum number of entries to maintain.
interval *interval*	(Optional) Specifies the sampling interval in seconds.
owner *owner*	(Optional) Specifies an owner for this entry.

Defaults

- If *buckets* is not specified, the maximum number of entries maintained will be 50.
- If not specified, *interval* will be set to 30 seconds.
- If *owner* is not specified, **monitor** will be applied.

Mode

Switch command, Read-Write.

Example

This example shows how configure RMON history entry 1 on port fe.2.1 to sample every 30 seconds:

```
Matrix(rw)->set rmon history 1 fe.2.1 interval 20
```

clear rmon history

Use this command to delete one or more RMON history entries or reset one or more entries to default values. For specific values, refer to “set rmon history” on page 11-19.

Syntax

clear rmon history {*index-list* | **to-defaults**}

Downloaded from www.Manualslib.com manuals search engine

Parameters

index-list	Specifies one or more history entries to be deleted, causing them to disappear from any future RMON queries.
to-defaults	Resets all history entries to default values. This will cause entries to reappear in RMON queries.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to delete RMON history entry 1:

```
Matrix(rw)->clear rmon history 1
```

show rmon alarm

Use this command to display RMON alarm entries.

Syntax

show rmon alarm [*index*]

Parameters

index	(Optional) Displays RMON alarm entries for a specific entry index ID.

Defaults

If *index* is not specified, information about all RMON alarm entries will be displayed.

Mode

Switch command, Read-Only.

Usage

The RMON alarm group periodically takes statistical samples from RMON variables and compares them with previously configured thresholds. If the monitored variable crosses a threshold an RMON event is generated.

Example

This example shows how to display RMON alarm entry 3:

```
Matrix(rw)->show rmon alarm 3
Index 3
---------------------
Owner               = Manager
Status              = valid
Variable            = 1.3.6.1.4.1.5624.1.2.29.1.2.1.0
```


Downloaded from www.Manualslib.com manuals search engine

```
Sample Type          = delta          Startup Alarm       = rising
Interval             = 30             Value               = 0
Rising Threshold     = 1              Falling Threshold   = 0
Rising Event Index   = 2              Falling Event Index = 0
```

Table 11-4 provides an explanation of the command output.

Table 11-4 show rmon alarm Output Details

Output...	What it displays...
Index	Index number for this alarm entry.
Owner	Text string identifying who configured this entry.
Status	Whether this event entry is enabled (valid) or disabled.
Variable	MIB object to be monitored.
Sample Type	Whether the monitoring method is an absolute or a delta sampling.
Startup Alarm	Whether alarm generated when this entry is first enabled is rising, falling, or either.
Interval	Interval in seconds at which RMON will conduct sample monitoring.
Rising Threshold	Minimum threshold for causing a rising alarm.
Falling Threshold	Maximum threshold for causing a falling alarm.
Rising Event Index	Index number of the RMON event to be triggered when the rising threshold is crossed.
Falling Event Index	Index number of the RMON event to be triggered when the falling threshold is crossed.

set rmon alarm properties

Use this command to configure an RMON alarm entry, or to create a new alarm entry with an unused alarm index number.

Syntax

set rmon alarm properties *index* [**interval** *interval*] [**object** *object*] [**type** {**absolute** | **delta**}] [**startup** {**rising** | **falling** | **either**}] [**rthresh** *rthresh*] [**fthresh** *fthresh*] [**revent** *revent*] [**fevent** *fevent*] [**owner** *owner*]

Parameters

index	Specifies an index number for this entry. Maximum number or entries is 50**.** Maximum value is **65535**.
interval *interval*	(Optional) Specifies an interval (in seconds) for RMON to conduct sample monitoring.
object *object*	(Optional) Specifies a MIB object to be monitored. **Note:** This parameter is not mandatory for executing the command, but must be specified in order to enable the alarm entry configuration.
type absolute | **delta**	(Optional) Specifies the monitoring method as: sampling the absolute value of the object, or the difference (delta) between object samples.

Downloaded from www.Manualslib.com manuals search engine

startup rising | **falling** | **either**	(Optional) Specifies the type of alarm generated when this event is first enabled as: • Rising - Sends alarm when an RMON event reaches a maximum threshold condition is reached, for example, more than 30 collisions per second. • Falling - Sends alarm when RMON event falls below a minimum threshold condition, for example when the network is behaving normally again. • Either - Sends alarm when either a rising or falling threshold is reached.
rthresh *rthresh*	(Optional) Specifies a minimum threshold for causing a rising alarm.
fthresh *fthresh*	(Optional) Specifies a maximum threshold for causing a falling alarm.
revent *revent*	(Optional) Specifies the index number of the RMON event to be triggered when the rising threshold is crossed.
fevent *fevent*	(Optional) Specifies the index number of the RMON event to be triggered when the falling threshold is crossed.
owner *owner*	(Optional) Specifies the name of the entity that configured this alarm entry.

Defaults

- interval - **3600** seconds
- type - **absolute**
- startup - **rising**
- rthresh - **0**
- fthresh - **0**
- revent - **0**
- fevent - **0**
- owner - **monitor**

Mode

Switch command, Read-Write.

Example

This example shows how to configure a rising RMON alarm. This entry will conduct monitoring of the delta between samples every 30 seconds:

```
Matrix(rw)->set rmon alarm properties 3 interval 30 object
   1.3.6.1.4.1.5624.1.2.29.1.2.1.0 type delta rthresh 1 revent 2 owner Manager
```

set rmon alarm status

Use this command to enable an RMON alarm entry.

Syntax

set rmon alarm status *index* **enable**

Downloaded from www.Manualslib.com manuals search engine

Parameters

index	Specifies an index number for this entry. Maximum number or entries is 50**.** Maximum value is **65535**.
enable	Enables this alarm entry.

Defaults

None.

Mode

Switch command, Read-Write.

Usage

An RMON alarm entry can be created using this command, configured using the **set rmon alarm properties** command ("set rmon alarm properties" on page 11-21), then enabled using this command. An RMON alarm entry can be created and configured at the same time by specifying an unused index with the set properties command.

An alarm is a notification that a statistical sample of a monitored variable has crossed a configured threshold.

Example

This example shows how to enable RMON alarm entry 3:

```
Matrix(rw)->set rmon alarm status 3 enable
```

clear rmon alarm

Use this command to delete an RMON alarm entry.

Syntax

clear rmon alarm *index*

Parameters

index	Specifies the index number of entry to be cleared.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to clear RMON alarm entry 1:

```
Matrix(rw)->clear rmon alarm 1
```


Downloaded from www.Manualslib.com manuals search engine

show rmon event

Use this command to display RMON event entry properties.

Syntax

show rmon event [*index*]

Parameters

index	(Optional) Displays RMON properties and log entries for a specific entry index ID.

Defaults

If *index* is not specified, information about all RMON entries will be displayed.

Mode

Switch command, Read-Only.

Example

This example shows how to display RMON event entry 3:

```
Matrix(rw)->show rmon event 3
Index 3
----------------
Owner          = Manager
Status         = valid
Description    = STP Topology change
Type           = log-and-trap
Community      = public
Last Time Sent = 0 days 0 hours 0 minutes 37 seconds
```

Table 11-5 provides an explanation of the command output.

Table 11-5 show rmon event Output Details

Output...	What it displays...
Index	Index number for this event entry.
Owner	Text string identifying who configured this entry.
Status	Whether this event entry is enabled (valid) or disabled.
Description	Text string description of this event.
Type	Whether the event notification will be a log entry, and SNMP trap, both, or none.
Community	SNMP community name if message type is set to trap.
Last Time Sent	When an event notification matching this entry was sent.

Downloaded from www.Manualslib.com manuals search engine

set rmon event properties

Use this command to configure an RMON event entry, or to create a new event entry with an unused event index number.

Syntax

set rmon event properties *index* [**description** *description*] [**type** {**none** | **log** | **trap** | **both**}] [**community** *community*] [**owner** *owner*]

Parameters

index	Specifies an index number for this entry. Maximum number of entries is 100. Maximum value is **65535**.
description *description*	(Optional) Specifies a text string description of this event.
type none | **log** | **trap** | **both**	(Optional) Specifies the type of RMON event notification as: none, a log table entry, an SNMP trap, or both a log entry and a trap message.
community *community*	(Optional) Specifies an SNMP community name to use if the message type is set to **trap**. For details on setting SNMP traps and community names, refer to "Configuring SNMP Target Addresses" on page 5-29.
owner *owner*	(Optional) Specifies the name of the entity that configured this entry.

Defaults

- If **description** is not specified, none will be applied.
- If not specified, **type none** will be applied.
- If *owner* is not specified, **monitor** will be applied.

Mode

Switch command, Read-Write.

Example

This example shows how to create and enable an RMON event entry called "STP topology change" that will send both a log entry and an SNMP trap message to the "public" community:

```
Matrix(rw)->set rmon event properties 2 description "STP topology change" type
both community public owner Manager
```

set rmon event status

Use this command to enable an RMON event entry. An event entry describes the parameters of an RMON event that can be triggered. Events can be fired by RMON alarms and can be configured to create a log entry, generate a trap, or both.

Syntax

set rmon event status *index* **enable**

Downloaded from www.Manualslib.com manuals search engine

Parameters

index	Specifies an index number for this entry. Maximum number of entries is 100. Maximum value is **65535**.
enable	Enables this event entry.

Defaults

None.

Mode

Switch command, Read-Write.

Usage

An RMON event entry can be created using this command, configured using the **set rmon event properties** command ("set rmon event properties" on page 11-25), then enabled using this command. An RMON event entry can be created and configured at the same time by specifying an unused index with the set properties command.

Example

This example shows how to enable RMON event entry 1:

```
Matrix(rw)->set rmon event status 1 enable
```

clear rmon event

Use this command to delete an RMON event entry and any associated log entries.

Syntax

clear rmon event *index*

Parameters

index	Specifies the index number of the entry to be cleared.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to clear RMON event 1:

```
Matrix(rw)->clear rmon event 1
```


Downloaded from www.Manualslib.com manuals search engine

show rmon host

Use this command to display RMON properties and statistics associated with each host discovered on the network.

Syntax

show rmon host [*port-string*] [**address** | **creation**]

Parameters

port-string	(Optional) Displays RMON properties and statistics for specific port(s).
address | **creation**	(Optional) Sorts the display by MAC address or creation time of the entry.

Defaults

- If *port-string* is not specified, information about all ports will be displayed.
- If **address** or **creation** are not specified, entries will not be sorted.

Mode

Switch command, Read-Only.

Example

This example shows how to display RMON host properties and statistics. A control entry displays first, followed by actual entries corresponding to the control entry. For a description of the types of statistics shown, refer to Table 11-3:

```
Matrix(rw)->show rmon host
------------------
Host Index     1
Interface      21009
Table size     100
Last deletion  766048
Status         1
Owner          monitor

Host 00-00-5e-00-01-01   Creation Order 22
In Pkts         0
Out Pkts        1
In Octets       0
Out Octets      66
Broadcast Pkts  0
Multicast Pkts  0

Host 00-00-f6-00-86-6d   Creation Order 74
In Pkts         0
Out Pkts        2
In Octets       0
```


Downloaded from www.Manualslib.com manuals search engine

```
Out Octets     136
Broadcast Pkts 0
Multicast Pkts 0
```

set rmon host properties

Use this command to configure an RMON host entry.

Syntax

set rmon host properties *index port-string* [*owner*]

Parameters

index	Specifies an index number for this entry. An entry will automatically be created if an unused index number is chosen. Maximum number of entries is 5. Maximum value is **65535**.
port-string	Configures RMON host monitoring on a specific port.
owner	(Optional) Specifies the name of the entity that configured this entry.

Defaults

If *owner* is not specified, **monitor** will be applied.

Mode

Switch command, Read-Write.

Example

This example shows how to configure RMON host entry 1 on Fast Ethernet port 5 in module 1:

```
Matrix(rw)->set rmon host properties 1 fe.1.5
```

set rmon host status

Use this command to enable an RMON host entry.

Syntax

set rmon host status *index* **enable**

Parameters

index	Specifies an index number for this entry. Maximum number of entries is 5. Maximum value is **65535**.
enable	Enables this host entry.

Defaults

None.

Mode

Switch command, Read-Write.

Downloaded from www.Manualslib.com manuals search engine

Example

This example shows how to enable RMON host entry 1:

```
Matrix(rw)->set rmon host status 1 enable
```

clear rmon host

Use this command to delete an RMON host entry.

Syntax

clear rmon host *index*

Parameters

index	Specifies the index number of the entry to be cleared.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to clear RMON host entry 1:

```
Matrix(rw)->clear rmon host 1
```

show rmon topN

Use this command to displays RMON TopN properties and statistics. TopN monitoring prepares tables that describe the hosts topping a list ordered by one of their statistics. TopN lists are samples of one of the hosts base statistics over a specific interval.

Syntax

set rmon topN [*index*]

Parameters

index	(Optional) Displays RMON properties and statistics for a specific entry index ID.

Defaults

If *index* is not specified, information about all entries will be displayed.

Mode

Switch command, Read-Only.

Downloaded from www.Manualslib.com manuals search engine

Example

This example shows how to display all RMON TopN properties and statistics. A control entry displays first, followed by actual entries corresponding to the control entry:

```
Matrix(rw)->show rmon topN
--------------------
Index           = 1
Status          = 1 valid
Owner           = monitor
Start Time      = 0
HostIndex       = 1
Rate Base       = 1 InPkts
Duration        = 10
Time Remaining  = 0
Requested Size  = 10000
Granted Size    = 100

Report 1
-------------------
Rate = 3
Address = 0.1.f4.6.2e.40
```

Table 11-6 provides an explanation of the command output. Properties are set using the **set rmon topN properties** command as described in "set rmon topN properties" on page 11-31.

Table 11-6 show rmon topN Output Details

Output...	What it displays...
Index	Index number for this event entry. Each entry defines one top N report prepared for one interface.
Status	Whether this event entry is enabled (valid) or disabled.
Owner	Text string identifying who configured this entry.
Start Time	System up time when this report was last started.
HostIndex	Index number of the host table for which this top N report will be prepared.
Rate Base	Type of counter (and corresponding integer value) activated with this entry: as InPackets (1), OutPackets (2), InOctets (3), OutOctets (4), OutErrors (5), Broadcast packets (6), or Multicast packets (7).
Duration	Collection time (in seconds) for this report.
Time Remaining	Collection time left for this report if still in progress.
Requested Size	Maximum number of hosts requested for the top N table.
Granted Size	Actual maximum number of hosts in the top N table. Depending on system resources, this may differ from the Requested Size value.
Rate	Amount of change in the counter type (InPackets, OutPackets, etc.) during the sampling interval.
Address	MAC address of the host.

Downloaded from www.Manualslib.com manuals search engine

set rmon topN properties

Use this command to configure an RMON topN entry (report).

Syntax

set rmon topn properties *index* [**hindex** *hindex*] [**rate** {**inpackets** | **outpackets** | **inoctets** | **outoctets** | **errors** | **bcast** | **mcast**}] [**duration** *duration*] [**size** *size*] [**owner** *owner*]

Parameters

index	Specifies an index number for this entry. An entry will automatically be created if an unused index number is chosen. Maximum number of entries is 10. Maximum value is **65535**.
hindex *hindex*	(Optional) Specifies an index number of the host table.
rate inpackets | **outpackets** | **inoctets** | **outoctets** | **errors** | **bcast** | **mcast**	(Optional) Specifies the type of counter to activate with this entry as InPackets, OutPackets, InOctets, OutOctets, OutErrors, Broadcast packets, or Multicast packets.
duration *duration*	(Optional) Specifies the sampling interval in seconds. Value must be a minimum of **60**.
size *size*	(Optional) Specifies the maximum number of entries to maintain.
owner *owner*	(Optional) Specifies the name of the entity that configured this entry.

Defaults

- If host index is not specified, none will be applied.
- If counter type is not specified, **inpackets** will be applied.
- If *duration* is not specified, none will be applied.
- If *size* is not specified, **10** will be applied.
- If *owner* is not specified, **monitor** will be applied.

Mode

Switch command, Read-Write.

Example

This example shows how to configure RMON TopN entry 1, for host 1 with a sampling interval of 60 seconds and a maximum number of entries of 20:

```
Matrix(rw)->set rmon topN properties 1 1 inpackets 60 20
```

set rmon topN status

Use this command to enable an RMON topN entry.

Syntax

set rmon topN status *index* **enable** |

Downloaded from www.Manualslib.com manuals search engine

Parameters

index	Specifies an index number for this entry. Maximum number of entries is 10. Maximum value is **65535**.
enable	Enables this TopN entry.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to enable RMON TopN entry 1:

```
Matrix(rw)->set rmon topN status 1 enable
```

clear rmon topN

Use this command to delete an RMON TopN entry.

Syntax

clear rmon topN *index*

Parameters

index	Specifies the index number of the entry to be cleared.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to delete RMON TopN entry 1:

```
Matrix(rw)->clear rmon topN 1
```

show rmon matrix

Use this command to display RMON matrix properties and statistics. The RMON matrix stores statistics for conversations between sets of two addresses.

Syntax

show rmon matrix [*port-string*] [**source** | **dest**]

Downloaded from www.Manualslib.com manuals search engine

Parameters

port-string	(Optional) Displays RMON properties and statistics for a specific port(s).
source | **dest**	(Optional) Sorts the display by source or destination address.

Defaults

- If *port-string* is not specified, information about all ports will be displayed.
- If not specified, information about source and destination addresses will be displayed.

Mode

Switch command, Read-Only.

Example

This example shows how to display RMON matrix properties and statistics. A control entry displays first, followed by actual entries corresponding to the control entry:

```
Matrix(rw)->show rmon matrix
------------------
Matrix Index    1
Interface       32009
Table size      100
Last deletion   116647
Status          1
Owner           monitor

Source      00-e0-63-9d-c1-c8    Destination 00-a0-c9-03-cd-7c
Packets   = 2                    Octets    = 286
Errors    = ---
```

Table 11-7 provides an explanation of the command output. Properties are set using the **set rmon matrix properties** command as described in "set rmon matrix properties" on page 11-34.

Table 11-7 show rmon matrix Output Details

Output...	What it displays...
Matrix Index	Index number for this RMON matrix entry.
Interface	Interface for which host monitoring is being conducted.
Table size	Number of entries in the matrix table for this interface.
Last deletion	System up time when the last entry was deleted from the matrix table associated with this entry.
Status	Whether this matrix entry is enabled (valid) or disabled.
Owner	Text string identifying who configured this entry.
Source	Source of the data from which this entry creates a traffic matrix.
Destination	Destination of the data from which this entry creates a traffic matrix.
Packets	Number of packets (including bad packets) transmitted from the source address to the destination address.

Downloaded from www.Manualslib.com manuals search engine

Table 11-7 show rmon matrix Output Details (continued)

Output...	What it displays...
Octets	Number of octets (excluding framing bits, but including FCS octets) contained in all packets transmitted from the source address to the destination address.
Errors	Errors recorded.

set rmon matrix properties

Use this command to configure an RMON matrix entry.

Syntax

set rmon matrix properties *index port-string* [*owner*]

Parameters

index	Specifies an index number for this entry. An entry will automatically be created if an unused index number is chosen. Maximum number of entries is 2. Maximum value is **65535**.
port-string	Specifies port(s) on which to monitors statistics.
owner	(Optional) Specifies the name of the entity that configured this entry.

Defaults

If *owner* is not specified, **monitor** will be applied.

Mode

Switch command, Read-Write.

Example

This example shows how to configure RMON matrix entry 1 for fe.1.1

```
Matrix(rw)->set rmon matrix properties 1 fe.1.1
```

set rmon matrix status

Use this command to enable an RMON matrix entry.

Syntax

set rmon matrix status *index* **enable**

Parameters

index	Specifies an index number for this entry. Maximum number of entries is 2. Maximum value is **65535**.
enable	Enables or disables this matrix entry.

Defaults

None.

Downloaded from www.Manualslib.com manuals search engine

Mode

Switch command, Read-Write.

Example

This example shows how to enable RMON matrix entry 1:

```
Matrix(rw)->set rmon matrix status 1 enable
```

clear rmon matrix

Use this command to delete an RMON matrix entry.

Syntax

clear rmon matrix *index*

Parameters

index	Specifies the index number of the entry to be cleared.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to delete RMON matrix entry 1:

```
Matrix(rw)->clear rmon matrix 1
```

show rmon channel

Use this command to display RMON channel entries for one or more ports.

Syntax

show rmon channel [*port-string*]

Parameters

port-string	(Optional) Displays RMON channel entries for a specific port(s).

Defaults

If *port-string* is not specified, information about all channels will be displayed.

Mode

Switch command, Read-Only.

Downloaded from www.Manualslib.com manuals search engine

Example

This example shows how to display RMON channel information for fe.2.12:

```
Matrix(rw)->show rmon channel fe.2.12
Port fe.2.12    Channel index= 628      EntryStatus= valid
-------------------------------------------------------
Control             off       AcceptType          matched
OnEventIndex        0         OffEventIndex       0
EventIndex          0         Status              ready
Matches             4498
Description         Thu Dec 16 12:57:32 EST 2004
Owner               NetSight smith
```

set rmon channel

Use this command to configure an RMON channel entry.

Syntax

set rmon channel *index port-string* [**accept** {**matched** | **failed**}] [**control** {**on** | **off**}] [**onevent** *onevent*] [**offevent** *offevent*] [**event** *event*] [**estatus** {**ready** | **fired** | **always**}] [**description** *description*] [**owner** *owner*]

Parameters

index	Specifies an index number for this entry. An entry will automatically be created if an unused index number is chosen. Maximum number of entries is 2. Maximum value is **65535**.
port-string	Specifies the port on which traffic will be monitored.
accept matched | **failed**	(Optional) Specifies the action of the filters on this channel as: • **matched** - Packets will be accepted on filter matches • **failed** - Packets will be accepted if they fail a match
control on | **off**	(Optional) Enables or disables control of the flow of data through the channel.
onevent *onevent*	(Optional) Specifies the index of the RMON event that will turn this channel on.
offevent *offevent*	(Optional) Specifies the index of the RMON event that will turn this channel off.
event *event*	(Optional) Specifies the event to be triggered when the channel is on and a packet is accepted
estatus ready | **fired** | **always**	(Optional) Specifies the status of the event as: • **ready** - A single event may be generated. • **fired** - No additional events may be generated. • **always** - An event will be generated for every match.
description *description*	(Optional) Specifies a description for this channel.
owner	(Optional) Specifies the name of the entity that configured this entry.

Downloaded from www.Manualslib.com manuals search engine

Defaults

- If an **action** is not specified, packets will be accepted on filter matches.
- If not specified, **control** will be set to **off**.
- If **onevent** and **offevent** are not specified, none will be applied.
- If event status is not specified, **ready** will be applied.
- If a **description** is not specified, none will be applied.
- If *owner* is not specified, it will be set to **monitor**.

Mode

Switch command, Read-Write.

Example

This example shows how to accept failed control on description “capture all”create an RMON channel entry:

```
Matrix(rw)->set rmon channel 54313 fe.2.12
```

clear rmon channel

Use this command to clear an RMON channel entry.

Syntax

clear rmon channel *index*

Parameters

index	Specifies the channel entry to be cleared.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to clear RMON channel entry 2:

```
Matrix(rw)->clear rmon channel 2
```

show rmon filter

Use this command to display one or more RMON filter entries.

Syntax

show rmon filter [**index** *index* | **channel** *channel*]

Downloaded from www.Manualslib.com manuals search engine

Parameters

index *index* | **channel** *channel*	(Optional) Displays information about a specific filter entry, or about all filters which belong to a specific channel.

Defaults

If no options are specified, information for all filter entries will be displayed.

Mode

Switch command, Read-Only.

Example

This example shows how to display all RMON filter entries and channel information:

```
Matrix(rw)->show rmon filter
Index= 55508    Channel Index= 628      EntryStatus= valid
------------------------------------------------------------
Data Offset          0          PktStatus           0
PktStatusMask        0          PktStatusNotMask    0
Owner                ETS,NAC-D
-----------------------------
Data
ff ff ff ff ff ff
-----------------------------
DataMask
ff ff ff ff ff ff
-----------------------------
DataNotMask
00 00 00 00 00 00
```

set rmon filter

Use this command to configure an RMON filter entry.

Syntax

set rmon filter *index channel_index* [**offset** *offset*] [**status** *status*] [**smask** *smask*] [**snotmask** *snotmask*] [**data** *data*] [**dmask** *dmask*] [**dnotmask** *dnotmask*] [**owner** *owner*]

Parameters

index	Specifies an index number for this entry. An entry will automatically be created if an unused index number is chosen. Maximum number of entries is 10. Maximum value is **65535**.
channel_index	Specifies the channel to which this filter will be applied.
offset *offset*	(Optional) Specifies an offset from the beginning of the packet to look for matches.
status *status*	(Optional) Specifies packet status bits that are to be matched.

Downloaded from www.Manualslib.com manuals search engine

smask *smask*	(Optional) Specifies the mask applied to status to indicate which bits are significant.
snotmask *snotmask*	(Optional) Specifies the inversion mask that indicates which bits should be set or not set
data *data*	(Optional) Specifies the data to be matched.
dmask *dmask*	(Optional) Specifies the mask applied to data to indicate which bits are significant.
dnotmask *dnotmask*	(Optional) Specifies the inversion mask that indicates which bits should be set or not set.
owner	(Optional) Specifies the name of the entity that configured this entry.

Defaults

- If *owner* is not specified, it will be set to **monitor**.
- If no other options are specified, none (0) will be applied.

Mode

Switch command, Read-Write.

Example

This example shows how to create RMON filter 1 and apply it to channel 9:

```
Matrix(rw)->set rmon filter 1 10 offset 30 data 0a154305 dmask ffffffff
```

clear rmon filter

Use this command to clear an RMON filter entry.

Syntax

clear rmon filter {**index** *index* | **channel** *channel*}

Parameters

index *index* | **channel** *channel*	Clears a specific filter entry, or all entries belonging to a specific channel.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to clear RMON filter entry 1:

```
Matrix(rw)->clear rmon filter index 1
```


Downloaded from www.Manualslib.com manuals search engine

show rmon capture

Use this command to display RMON capture entries and associated buffer control entries.

Syntax

show rmon capture [*index*] [**nodata**]

Parameters

index	(Optional) Displays the specified buffer control entry and all captured packets associated with that entry.
nodata	(Optional) Displays only the buffer control entry specified by index.

Defaults

If no options are specified, all buffer control entries and associated captured packets will be displayed.

Mode

Switch command, Read-Only.

Example

This example shows how to display RMON capture entries and associated buffer entries:

```
Matrix(rw)->show rmon capture
Buf.control= 28062  Channel= 38283      EntryStatus= valid
------------------------------------------------------------
FullStatus          avail     FullAction          lock
Captured packets    251       Capture slice       128
Download size       100       Download offset     0
Max Octet Requested 50000     Max Octet Granted   50000
Start time          1 days 0 hours 51 minutes 15 seconds
Owner               monitor


captureEntry= 1        Buff.control= 28062
-------------------------------------------
Pkt ID      9         Pkt time    1 days 0 hours 51 minutes 15 seconds
Pkt Length  93        Pkt status  0
Data:
00 00 5e 00 01 01 00 01 f4 00 7d ce 08 00 45 00
00 4b b4 b9 00 00 40 11 32 5c 0a 15 43 05 86 8d
bf e5 00 a1 0e 2b 00 37 cf ca 30 2d 02 01 00 04
06 70 75 62 6c 69 63 a2 20 02 02 0c 92 02 01 00
02 01 00 30 14 30 12 06 0d 2b 06 01 02 01 10 07
01 01 0b 81 fd 1c 02 01 01 00 11 0b 00
```


Downloaded from www.Manualslib.com manuals search engine

set rmon capture

Use this command to configure an RMON capture entry, or to enable or disable an existing entry.

Syntax

set rmon capture *index* {*channel* [**action** {**lock** | **wrap**}] [**slice** *slice*] [**loadsize** *loadsize*] [**offset** *offset*] [**asksize** *asksize*] [**owner** *owner*]} | {**enable** | **disable**}

Parameters

index	Specifies a buffer control entry.
channel	Specifies the channel to which this capture entry will be applied.
action lock | **wrap**	(Optional) Specifies the action of the buffer when it is full as: • **lock** - Packets will cease to be accepted • **wrap** - Oldest packets will be overwritten
slice *slice*	(Optional) Specifies the maximum octets from each packet to be saved in a buffer. (default: 100)
loadsize *loadsize*	(Optional) Specifies the maximum octets from each packet to be downloaded from the buffer (default: 100)
offset *offset*	(Optional) Specifies that the first octet from each packet that will be retrieved.
asksize *asksize*	(Optional) Specifies that the requested maximum octets will be saved in this buffer.
owner	(Optional) Specifies the name of the entity that configured this entry.
enable | **disable**	Enables or disables an existing RMON capture entry.

Defaults

- If not specified, **action** defaults to **lock**.
- If not specified, offset defaults to **0**.
- If not specified, asksize defaults to **1** (which will request as many octets as possible)
- If **slice** and **loadsize** are not specified, **100** will be applied.
- If *owner* is not specified, it will be set to **monitor**.

Mode

Switch command, Read-Write.

Example

This example shows how to create RMON capture entry 1 to “listen” on channel 628:

```
Matrix(rw)->set rmon capture 1 628
```


Downloaded from www.Manualslib.com manuals search engine

clear rmon capture

Use this command to clears an RMON capture entry.

Syntax

clear rmon capture *index*

Parameters

index	Specifies the capture entry to be cleared.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to clear RMON capture entry 1:

```
Matrix(rw)->clear rmon capture 1
```


Downloaded from www.Manualslib.com manuals search engine

12

Network Address and Route Management Configuration

This chapter describes switch-related network address and route management commands and how to use them.

Note: The commands in this section pertain to the Enterasys Matrix Series device from the **switch CLI** only. For information on router-related network management tasks, including reviewing router ARP tables and IP traffic, refer to Chapter 16.

Managing Switch Network Addresses and Routes

Purpose

To display, add or delete switch ARP table entries, to enable or disable RAD (Runtime Address Discovery) protocol, to display, add or delete IP routing table addresses, and to display MAC address information.

Commands

For information about...	Refer to page...
show arp	12-2
set arp	12-3
clear arp	12-3
show rad	12-4
set rad	12-4
show ip route	12-5
traceroute	12-6
set ip route	12-8
clear ip route	12-8
show port mac	12-9
show mac	12-10
set mac	12-11
clear mac	12-12

Downloaded from www.Manualslib.com manuals search engine

For information about...	Refer to page...
show newaddrtraps	12-13
set newaddrtraps	12-14
show movedaddrtrap	12-14
set movedaddrtrap	12-15

show arp

Use this command to display the switch's ARP table.

Syntax

show arp

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Only.

Example

This example shows how to display the ARP table:

```
Matrix(rw)->show arp

LINK LEVEL ARP TABLE
IP Address       Phys Address       Flags   Interface
-------------------------------------------------------
10.20.1.1        00-00-5e-00-01-1   S       host0
134.142.21.194   00-00-5e-00-01-1   S       host0
134.142.191.192  00-00-5e-00-01-1   S       host0
134.142.192.18   00-00-5e-00-01-1   S       host0
134.142.192.119  00-00-5e-00-01-1   S       host0
-------------------------------------------------------
```

Table 12-1 provides an explanation of the command output.

Downloaded from www.Manualslib.com manuals search engine

Table 12-1 show arp Output Details

Output...	What it displays...
IP Address	IP address mapped to MAC address.
Phys Address	MAC address mapped to IP address.
Flags	Route status. Possible values and their definitions include: **S** - manually configured entry (static) **P** - respond to ARP requests for this entry

set arp

Use this command to add mapping entries to the switch's ARP table.

Syntax

set arp *ip-address mac-address* [{**temp** | **pub** | **trail**}]

Parameters

ip-address	Specifies the IP address to map to the MAC address and add to the ARP table.
mac-address	Specifies the MAC address to map to the IP address and add to the ARP table.
temp	(Optional) Sets the ARP entry as not permanent. This allows the entry to time out.
pub	(Optional) Publishes the specified ARP entry. This causes the system to respond to ARP requests for this entry, even though it is not the host.
trail	(Optional) Specifies that trailer encapsulations can be sent to this host.

Defaults

- If **temp** is not specified, the ARP entry will be added as a permanent entry.
- If **pub** is not specified, then the ARP entry will not be published.
- If **trail** is not specified, then trailer encapsulations will not be sent to the host.

Mode

Switch command, Read-Write.

Example

This example shows how to map IP address 198.133.219.232 to MAC address 00-00-0c-40-0f-bc:

```
Matrix(rw)->set arp 198.133.219.232 00-00-0c-40-0f-bc
```

clear arp

Use this command to delete a specific entry or all entries from the switch's ARP table.

Syntax

clear arp {*ip* | **all**}

Downloaded from www.Manualslib.com manuals search engine

Parameters

ip | **all**	Specifies the IP address in the ARP table to be cleared, or clears all ARP entries.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to delete entry 10.1.10.10 from the ARP table:

```
Matrix(rw)->clear arp 10.1.10.10
```

show rad

Use this command to display the status of the RAD (Runtime Address Discovery) protocol on the switch.

Syntax

show rad

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Only.

Example

This example shows how to display RAD status:

```
Matrix(rw)->show rad
 RAD is currently enabled.
```

set rad

Use this command to enable or disable RAD (Runtime Address Discovery) protocol.

Syntax

set rad {**enable** | **disable**}

Parameters

enable | **disable**	Enables or disables RAD.

Downloaded from www.Manualslib.com manuals search engine

Defaults

None.

Mode

Switch command, Read-Write.

Usage

The Enterasys Matrix Series device uses BOOTP/DHCP to obtain an IP address if one hasn't been configured. RAD can also be used to retrieve a text configuration file from the network.

In order for RAD to retrieve a text configuration file, the file must be specified in the BootP tab.

RAD on DFE devices will only accept an address from a DHCP or BootP server if the lease time for the address is set to infinity (unlimited). This will prevent the DFE from switching addresses when a lease time expires.

Example

This example shows how to disable RAD:

```
Matrix(rw)->set rad disable
```

show ip route

Use this command to display the switch's IP routing table entries.

Syntax

show ip route

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Only.

Example

This example shows how to display the IP routing table:

```
Matrix(rw)->show ip route

ROUTE TABLE
Destination      Gateway         Mask      TOS  Flags Refcnt Use      Interface
-------------------------------------------------------------------------------
default         12.22.73.13      00000000  0    UC    0      0       host0
10.0.0.0        12.22.73.13      ff000000  0    UC          0       host0
127.0.0.1       127.0.0.1        00000000  0    UH    0      104     lo0
```

Table 12-2 provides an explanation of the command output.

Downloaded from www.Manualslib.com manuals search engine

Table 12-2 show ip route Output Details

Output...	What it displays...
Destination	IP address of the host entry.
Gateway	MAC address of the destination.
Mask	IP mask of the destination.
TOS	Type of Service setting.
Flags	Route status. Possible values and their definitions include: **U** - route is usable (that is, "up") **G** - destination is a gateway **H** - host specific routing entry **R** - host or net unreachable D - created dynamically (by redirect) **M** - modified dynamically (by redirect) **d** - message confirmed **C** - generate new routes on use **X** - external daemon resolves name **L** - generated by ARP **S** - manually added (static) **1** - protocol specific routing flag **2** - protocol specific routing flag
Refcnt	Number of hosts referencing this address.
Use	Number of packets forwarded via this route.
Interface	Interface type.

traceroute

Use this command to display a hop-by-hop path through an IP network from the device to a specific destination host.

Syntax

traceroute [**-w** *waittime*] [**-f** *first-ttl*] [**-m** *max-ttl*] [**-p** *port*] [**-q** *nqueries*] [**-s** *src-addr*] [**-r**] [**-d**] [**-t** *tos*] [**-F**] [**-g** *gateway*] [**-I**] [**-n**] [**-v**] [**-x**] *host* [*packetlen*]

Parameters

-w *waittime*	(Optional) Specifies time in seconds to wait for a response to a probe.
-f *first-ttl*]	(Optional) Specifies the time to live (TTL) of the first outgoing probe packet.
-m *max-ttl*	(Optional) Specifies the maximum time to live (TTL) used in outgoing probe packets.
-p *port*	(Optional) Specifies the base UDP port number used in probes.
-q *nqueries*	(Optional) Specifies the number of probe inquiries.
-s *src-addr*	(Optional?) Specifies the source IP address to use in outgoing probe packets.
-r	(Optional) Bypasses the normal host routing tables.

Downloaded from www.Manualslib.com manuals search engine

-d	(Optional) Sets the debug socket option.
-t *tos*	(Optional) Sets the type of service (TOS) to be used in probe packets.
-F	(Optional) Sets the 'don't fragment' bit.
-g *gateway*	(Optional) Specifies a loose source gateway (up to 8 can be specified), or specifies a specific gateway, such as **gw1**.
-I	(Optional) Specifies the use of ICMP echo requests rather than UDP datagrams.
-n	(Optional) Displays hop addresses numerically. (Supported in a future release.)
-v	(Optional) Displays verbose output, including the size and destination of each response.
-x	(Optional) Prevents traceroute from calculating checksums.
host	Specifies the host to which the route of an IP packet will be traced.
packetlen	(Optional) Specifies the length of the probe packet.

Defaults

- If not specified, *waittime* will be set to **5** seconds.
- If not specified, *first-ttl* will be set to **1** second.
- If not specified, *max-ttl* will be set to **30** seconds.
- If not specified, *port* will be set to **33434**.
- If not specified, *nqueries* will be set to **3**.
- If **-r** is not specified, normal host routing tables will be used.
- If **-d** is not specified, the debug socket option will not be used.
- If not specified, *tos* will be set to **0**.
- If **-F** is not specified, the 'don't fragment' bit will not be applied.
- If *gateway* is not specified, none will be applied.
- If **-I** is not specified, UDP datagrams will be used.
- If **-v** is not specified, summary output will be displayed.
- If **-x** is not specified, checksums will be calculated.

Mode

Switch command, Read-Only.

Usage

Three UDP or ICMP probes will be transmitted for each hop between the source and the traceroute destination.

Downloaded from www.Manualslib.com manuals search engine

Example

This example shows how to use traceroute to display a round trip path to host 192.167.252.17. In this case, hop 1 is the Enterasys Matrix Series switch, hop 2 is 14.1.0.45, and hop 3 is back to the host IP address. Round trip times for each of the three UDP probes are displayed next to each hop:

```
Matrix(rw)->traceroute 192.167.252.17
traceroute to 192.167.252.17 (192.167.252.17), 30 hops max, 40 byte packets
  1  matrix.enterasys.com (192.167.201.40)  20.000 ms  20.000 ms  20.000 ms
  2  14.1.0.45 (14.1.0.45)  40.000 ms  10.000 ms  20.000 ms
  3  192.167.252.17 (192.167.252.17)  50.000 ms  0.000 ms  20.000 ms
```

set ip route

Use this command to add a route to the switch's IP routing table.

Syntax

set ip route {*destination* | **default**} *gateway*

Parameters

destination	Specifies the IP address of the network or host to be added.
default	Sets the default gateway.
gateway	Specifies the IP address of the next-hop device.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to add an IP route from 192.122.173.42 to 192.122.168.38 to the routing table:

```
Matrix(rw)->set ip route 192.122.173.42 192.122.168.38
```

clear ip route

Use this command to delete switch IP routing table entries.

Syntax

clear ip route *destination* | **default**

Parameters

destination	Specifies the IP address of the network or host to be cleared.
default	Clears the default gateway.

Downloaded from www.Manualslib.com manuals search engine

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to clear the default gateway:

```
Matrix(rw)->clear ip route default
```

show port mac

Use this command to display the MAC address(es) for one or more ports.

Syntax

show port mac [*port-string*]

Parameters

port-string	(Optional) Displays MAC addresses for specific port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.

Defaults

If *port-string* is not specified, MAC addresses for all ports will be displayed.

Mode

Switch command, Read-Only.

Usage

These are port MAC addresses programmed into the device during manufacturing. To show the MAC addresses learned on a port through the switching process, use the **show mac** command as described in "show mac" on page 12-10.

Example

This example shows how to display the MAC address for 1-Gigabit Ethernet port 4 in module 2:

```
Matrix(rw)->show port mac fe.2.4

Port            MAC Address
------------  ----------------------
fe.2.4        00-01-F4-DA-32-FE
```


Downloaded from www.Manualslib.com manuals search engine

show mac

Use this command to display the timeout period for aging learned MAC addresses, and to show MAC addresses in the switch's filtering database.

Syntax

show mac [**agetime**] [**address** *mac-address*] [**fid** *fid*] [**vlan-id** *vlan-id*] [**port-string** *port-string*] [**type** {**other** | **invalid** | **learned** | **self** | **mgmt**}] [**field-decode**] [**unicast-as-multicast**] [**-verbose**]

Parameters

agetime	(Optional) Display the time in seconds that a learned MAC address will stay in the filtering database.
address *mac-address*	(Optional) Displays a specific MAC address (if it is known by the device).
fid *fid*	(Optional) Displays MAC addresses for a specific filter database identifier.
vlan-id *vlan-id*	(Optional) Displays MAC addresses for a specific VLAN based on the VLAN ID, for static multicast entries only.
port-string *port-string*	(Optional) Displays MAC addresses for a specific port or range of ports. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.
type other | **invalid** | **learned** | **self** | **mgmt**	(Optional) Display MAC addresses defined as **other**, **invalid**, **learned**, **self** or **mgmt** (management).
field-decode	(Optional) Display the meanings of the fields in the **show mac** command.
unicast-as-multicast	(Optional) Display matches of unlearned destination MAC address against the static multicast MAC entries.
-verbose	(Optional) Displays all MAC address information in detail.

Defaults

If no parameters are specified, all MAC addresses for the device will be displayed.

Mode

Switch command, Read-Only.

Usage

These are addresses learned on a port through the switching process or statically entered. To show port MAC addresses programmed into the device during manufacturing, use the **show port mac** command as described in "show port mac" on page 12-9.

Examples

This example shows how to display the MAC address timeout period:

```
Matrix(rw)->show mac agetime
Aging time: 300 seconds
```

This example shows how to display MAC address information for Fast Ethernet port 3 in module 1:

Downloaded from www.Manualslib.com manuals search engine

```
Matrix(rw)->show mac port-string fe.1.3

MAC Address       FID  Port          Type    Status
----------------- ---- ------------- ------- -------
00-01-F4-32-88-C5 0    fe.1.3        self
00-00-1D-12-11-88 3    fe.1.3        mgmt    perm
```

Table 12-3 provides an explanation of the command output.

Table 12-3 show mac Output Details

Output...	What it displays...
MAC Address	MAC addresses mapped to the port(s) shown.
FID	Filter database identifier.
Port	Port designation.
Type	Address type. Valid types are: • other - entry is other than below • invalid - entry is no longer valid, but has not been yet flushed-out • learned - entry has been learned and is currently used • self - entry represents one of the device's address • mgmt - entry represents a dot1qStaticUnicastAddress (manually entered MAC address) • mcast - entry represents a dot1qStaticMulticastAddress
Status	Address status. Valid types are: • other - entry is other than below • invalid - entry shall be removed • perm - entry is currently in use and shall remain so AFTER the next reset (permanent)

set mac

Use this command to set the timeout period for aging learned MAC entries, to define what ports a multicast address can be dynamically learned on or flooded to, and to make a static entry into the filtering database(s).

Syntax

set mac [**agetime** *time*] | [**multicast** *mac-address vlan-id* [*port-string*] {**append** | **clear**}] | [**unicast** *mac-address fid receive-port* [**ageable**]] [**unicast-as-multicast** {**enable** | **disable**}]

Parameters

agetime *time*	Specifies the timeout period in seconds for aging learned MAC addresses. Valid values are **10** to **65535**.
multicast *mac-address vlan-id* [*port-string*] {**append** | **clear**}]	This command allows you to limit specific layer two multicast addresses (*mac-address*) to specific ports (*port-string*) within a VLAN (*vlan-id*). You can later come back and **append** or **clear** ports from the list of ports the multicast MAC address is allowed to be dynamically learned on or flooded to.

Downloaded from www.Manualslib.com manuals search engine

unicast *mac-address fid receive-port* [**ageable**]	This command allows you to statically enter a unicast MAC address (*mac-address*) into a filtering database (*fid*) for a single port (*receive-port*). This entry will be either permanent or **ageable** where it will age out same as a dynamically learned MAC address.
unicast-as-multicast {**enable** | **disable**}	(Optional) **enable** - Enables treating static unicast MAC address as a multicast address by extending the search phase of layer 2 lookup to match the unlearned destination MAC address against the static Multicast MAC entries. **disable** - Treats static unicast MAC addresses as unicast addresses.

Defaults

If port-string is not defined with the **set mac multicast** command, then it will apply to all ports.

If the **set mac unicast** command is used without the **ageable** parameter, the entry will be permanent.

Mode

Switch command, Read-Write.

Usage

A warning displays if a unicast MAC address is entered as part of a multicast command:

matrix(rw)->**set mac multicast 00-02-ca-bb-cc-dd 2 fe.1.5**

Warning: Unicast address converted to multicast 01-02-CA-BB-CC-DD

Example

This example shows how to set the MAC timeout period to 600 seconds:

```
Matrix(rw)->set mac agetime 600
```

This example shows how to enable the MAC for unicast-as-multicast:

```
Matrix(rw)->set mac unicast-as-multicast enable
```

clear mac

Use this command to reset the timeout period for aging learned MAC entries to the default value of 300 seconds, or to clear MAC addresses out of the filtering database(s).

Syntax

clear mac {[**all**] | [**address** *address*] [**fid** *fid*] | [**vlan-id** *vlan-id*] | [**port-string** *port-string*] [**type** {**learned** | **mgmt**}]} | [**agetime**] [**unicast-as-multicast**]

Parameters

all	Clear all MAC address entries. This will even clear permanent entries.
address *address*	MAC address to clear (ex. 00-01-F4-56-78-90); if not specified, clear command shall be scoped to all MAC address.
fid *fid*	Filtering database id to clear; if not specified, clear command shall be scoped to all filtering database ids.

Downloaded from www.Manualslib.com manuals search engine

vlan-id *vlan-id*	Specify a VLAN ID from which to clear the MAC address for static multicast entries only.
port-string *port-string*	Single port to clear (ex. fe.1.1); if not specified, clear command shall be scoped to all ports.
type {**learned** | **mgmt**}	Status type to clear; if not specified, clear command shall be scoped to all 'learned' and 'mgmt' entries where mgmt refers to all statically entered MAC addresses.
agetime	(Optional) Clear timeout period to default value of 300 seconds.
unicast-as-multicast	(Optional) The layer 2 lookup to attempt to match the unlearned destination MAC address against the static multicast MAC entries cleared.

Parameters

None.

Defaults

None, except those noted above.

Mode

Switch command, Read-Write.

Examples

This example shows how to clear the MAC timeout period:

```
Matrix(rw)->clear mac agetime
```

This example shows how to clear all the MAC addresses associated with port fe.1.3:

```
Matrix(rw)->clear mac port-string fe.1.3
```

show newaddrtraps

Use this command to display the status of MAC address traps on one or more ports.

Syntax

show newaddrtrap [*port-string*]

Parameters

port-string	(Optional) Displays MAC address traps for specific port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.

Defaults

If *port-string* is not specified, MAC address traps for all ports will be displayed.

Mode

Switch command, Read-Only.

Downloaded from www.Manualslib.com manuals search engine

Example

This example shows how to display the status of MAC address traps on ge.1.1 through 3:

```
Matrix(rw)->show newaddrtrap
New Address Traps Globally disabled

Port        Enable State
--------- ------------
ge.1.1    disabled
ge.1.2    disabled
ge.1.3    disabled
```

set newaddrtraps

Use this command to enable or disable SNMP trap messaging, globally or on one or more ports, when new source MAC addresses are detected.

Syntax

set newaddrtrap [*port-string*] {**enable** | **disable**}

Parameters

port-string	(Optional) Specifies the port(s) on which to enable or disable MAC address traps. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.
enable | **disable**	Enables or disables SNMP trap messaging when new source MAC addresses are detected.

Defaults

If *port-string* is not specified, MAC address traps will be globally enabled or disabled.

Mode

Switch command, Read-Write.

Example

This example shows how to globally enable MAC address traps:

```
Matrix(rw)->set newaddrtrap enable
```

show movedaddrtrap

Use this command to display the status of moved MAC address traps on one or more ports.

Syntax

show movedaddrtrap [*port-string*]

Downloaded from www.Manualslib.com manuals search engine

Parameters

port-string	(Optional) Displays MAC address traps for specific port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.

Defaults

If *port-string* is not specified, MAC address traps for all ports will be displayed.

Mode

Switch command, Read-Only.

Example

This example shows how to display the status of MAC address traps on ge.1.1 through 3:

```
Matrix(rw)->show movedaddrtrap ge.1.1-3
Moved Address Traps Globally enabled

Port        Enable State
--------- ------------
ge.1.1     enabled
ge.1.2     enabled
ge.1.3     enabled
```

set movedaddrtrap

Use this command to enable or disable SNMP trap messaging, globally or on one or more ports, when moved source MAC addresses are detected.

Syntax

set movedaddrtrap [*port-string*] {**enable** | **disable**}

Parameters

port-string	(Optional) Specifies the port(s) on which to enable or disable MAC address traps. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.
enable | **disable**	Enables or disables SNMP trap messaging when moved source MAC addresses are detected.

Defaults

If *port-string* is not specified, MAC address traps will be globally enabled or disabled.

Mode

Switch command, Read-Write.

Downloaded from www.Manualslib.com manuals search engine

Example

This example shows how to globally enable MAC address traps:

```
Matrix(rw)->set movedaddrtrap enable
```


Downloaded from www.Manualslib.com manuals search engine

13

SNTP Configuration

This chapter describes Simple Network Time Protocol (SNTP) commands and how to use them.

Configuring Simple Network Time Protocol (SNTP)

Purpose

To configure the Simple Network Time Protocol (SNTP), which synchronizes device clocks in a network.

Commands

For information about...	Refer to page...
show sntp	13-2
set sntp client	13-3
clear sntp client	13-4
set sntp server	13-4
clear sntp server	13-5
set sntp broadcastdelay	13-5
clear sntp broadcast delay	13-6
set sntp poll-interval	13-6
clear sntp poll-interval	13-7
set sntp poll-retry	13-7
clear sntp poll-retry	13-7
set sntp poll-timeout	13-8
clear sntp poll-timeout	13-8
show timezone	13-9
set timezone	13-9
clear timezone	13-10

Downloaded from www.Manualslib.com manuals search engine

show sntp

Use this command to display SNTP client settings.

Syntax

show sntp

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Only.

Example

This example shows how to display SNTP client settings:

```
Matrix(rw)->show sntp
SNTP Version: 3
Current Time: TUE SEP 09 16:13:33 2003
Timezone: 'EST', offset from UTC is -4 hours and 0 minutes
Client Mode: unicast
Broadcast Delay: 3000 microseconds
Broadcast Count: 0
Poll Interval: 512 seconds
Poll Retry: 1
Poll Timeout: 5 seconds
SNTP Poll Requests: 1175
Last SNTP Update: TUE SEP 09 16:05:24 2003
Last SNTP Request: TUE SEP 09 16:05:24 2003
Last SNTP Status: Success

SNTP-Server       Precedence       Status
-----------------------------------------
10.2.8.6              2            Active
144.111.29.19         1            Active
```

Table 13-1 provides an explanation of the command output.

Table 13-1 show sntp Output Details

Output...	What it displays...
SNTP Version	SNTP version number.
Current Time	Current time on the system clock.
Timezone	Time zone name and amount it is offset from UTC (Universal Time). Set using **set timezone** command (“set timezone” on page 13-9).

Downloaded from www.Manualslib.com manuals search engine

Table 13-1 show sntp Output Details (continued)

Output...	What it displays...
Client Mode	Whether SNTP client is operating in unicast or broadcast mode. Set using **set sntp client** command ("set sntp client" on page 13-3).
Broadcast Delay	Round trip delay for SNTP broadcast frames. Default of 3000 microseconds can be reset using the **set sntp broadcastdelay** command ("set sntp broadcastdelay" on page 13-5).
Broadcast Count	Number of SNTP broadcast frames received.
Poll Interval	Interval between SNTP unicast requests. Default of 512 seconds can be reset using the **set sntp poll-interval** command ("set sntp poll-interval" on page 13-6).
Poll Retry	Number of poll retries to a unicast SNTP server. Default of 1 can be reset using the **set sntp poll-retry** command ("set sntp poll-retry" on page 13-7).
Poll Timeout	Timeout for a response to a unicast SNTP request. Default of 5 seconds can be reset using **set sntp poll-timeout** command ("clear sntp poll-timeout" on page 13-8).
SNTP Poll Requests	Total number of SNTP poll requests.
Last SNTP Update	Date and time of most recent SNTP update.
Last SNTP Request	Date and time of most recent SNTP update.
Last SNTP Status	Whether or not broadcast reception or unicast transmission and reception was successful.
SNTP-Server	IP address(es) of SNTP server(s).
Precedence	Precedence level of SNTP server in relation to its peers. Highest precedence is 1 and lowest is 10. Default of 1 can be reset using the **set sntp server** command ("set sntp server" on page 13-4).
Status	Whether or not the SNTP server is active.

set sntp client

Use this command to set the SNTP operation mode.

Syntax

```
set sntp client {broadcast | unicast | disable}
```

Parameters

broadcast	Enables SNTP in broadcast client mode.
unicast	Enables SNTP in unicast (point-to-point) client mode. In this mode, the client must supply the IP address from which to retrieve the current time.
disable	Disables SNTP.

Defaults

None.

Downloaded from www.Manualslib.com manuals search engine

Mode

Switch command, Read-Write.

Example

This example shows how to enable SNTP in broadcast mode:

```
Matrix(rw)->set sntp client broadcast
```

clear sntp client

Use this command to clear the SNTP client's operational mode.

Syntax

clear sntp client

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to clear the SNTP client's operational mode:

```
Matrix(rw)->clear sntp client
```

set sntp server

Use this command to add a server from which the SNTP client will retrieve the current time when operating in unicast mode. Up to 10 servers can be set as SNTP servers.

Syntax

set sntp server *ip-address* [*precedence*]

Parameters

ip-address	Specifies the SNTP server's IP address.
precedence	(Optional) Specifies this SNTP server's precedence in relation to its peers. Valid values are **1** (highest) to **10** (lowest).

Defaults

If *precedence* is not specified, 1 will be applied.

Mode

Switch command, Read-Write.

Downloaded from www.Manualslib.com manuals search engine

Example

This example shows how to set the server at IP address 10.21.1.100 as an SNTP server:

```
Matrix(rw)->set sntp server 10.21.1.100
```

clear sntp server

Use this command to remove one or all servers from the SNTP server list.

Syntax

clear sntp server {*ip-address* | **all**}

Parameters

ip-address	Specifies the IP address of a server to remove from the SNTP server list.
all	Removes all servers from the SNTP server list.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to remove the server at IP address 10.21.1.100 from the SNTP server list:

```
Matrix(rw)->clear sntp server 10.21.1.100
```

set sntp broadcastdelay

Use this command to set the round trip delay, in microseconds, for SNTP broadcast frames.

Syntax

set sntp broadcastdelay *time*

Parameters

time	Specifies broadcast delay time in microseconds. Valid values are **1** to **999999**. Default value is **3000**.

Defaults

None.

Mode

Switch command, Read-Write.

Downloaded from www.Manualslib.com manuals search engine

Example

This example shows how to set the SNTP broadcast delay to 12000 microseconds:

```
Matrix(rw)->set sntp broadcastdelay 12000
```

clear sntp broadcast delay

Use this command to clear the round trip delay time for SNTP broadcast frames.

Syntax

clear sntp broadcastdelay

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to clear the SNTP broadcast delay time:

```
Matrix(rw)->clear sntp broadcastdelay
```

set sntp poll-interval

Use this command to set the poll interval between SNTP unicast requests.

Syntax

set sntp poll-interval *interval*

Parameters

interval	Specifies the poll interval in seconds. Valid values are **16** to **16284**.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to set the SNTP poll interval to 30 seconds:

```
Matrix(rw)->set sntp poll-interval 30
```


Downloaded from www.Manualslib.com manuals search engine

clear sntp poll-interval

Use this command to clear the poll interval between unicast SNTP requests.

Syntax

clear sntp poll-interval

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to clear the SNTP poll interval:

```
Matrix(rw)->clear sntp poll-interval
```

set sntp poll-retry

Use this command to set the number of poll retries to a unicast SNTP server.

Syntax

set sntp poll-retry *retry*

Parameters

retry	Specifies the number of retries. Valid values are **0** to **10.**

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to set the number of SNTP poll retries to 5:

```
Matrix(rw)->set sntp poll-retry 5
```

clear sntp poll-retry

Use this command to clear the number of poll retries to a unicast SNTP server.

Syntax

clear sntp poll-retry

Downloaded from www.Manualslib.com manuals search engine

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to clear the number of SNTP poll retries:

```
Matrix(rw)->clear sntp poll-retry
```

set sntp poll-timeout

Use this command to set the poll timeout (in seconds) for a response to a unicast SNTP request.

Syntax

set sntp poll-timeout *timeout*

Parameters

timeout	Specifies the poll timeout in seconds. Valid values are **1** to **30**.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to set the SNTP poll timeout to 10 seconds:

```
Matrix(rw)->set sntp poll-timeout 10
```

clear sntp poll-timeout

Use this command to clear the SNTP poll timeout.

Syntax

clear sntp poll-timeout

Parameters

None.

Defaults

None.

Downloaded from www.Manualslib.com manuals search engine

Mode

Switch command, Read-Write.

Example

This example shows how to clear the SNTP poll timeout:

```
Matrix(rw)->clear sntp poll-timeout
```

show timezone

Use this command to display SNTP time zone settings.

Syntax

show timezone

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Only.

Example

This example shows how to display SNTP time zone settings:

```
Matrix(rw)->show timezone
Admin Config timezone: '', offset from UTC is 5 hours and 0 minutes
Oper  Config timezone: '', offset from UTC is 5 hours and 0 minutes
```

set timezone

Use this command to set the SNTP time zone name and the hours and minutes it is offset from Coordinated Universal Time (UTC).

Syntax

set timezone *name* [*hours*] [*minutes*]

Parameters

name	Specifies the time zone name.
hours	(Optional) Specifies the number of hours this timezone will be offset from UTC. Valid values are minus 12 (**-12**) to **12**.
minutes	(Optional) Specifies the number of minutes this timezone will be offset from UTC. Valid values are **0** to **59**.

Downloaded from www.Manualslib.com manuals search engine

Defaults

If offset *hours* or *minutes* are not specified, none will be applied.

Mode

Switch command, Read-Write.

Example

This example shows how to set the time zone to EST with an offset of minus 5 hours:

```
Matrix(rw)->set timezone ETS -5 0
```

clear timezone

Use this command to remove SNTP time zone adjustment values.

Syntax

`clear timezone`

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to remove SNTP time zone adjustment values:

```
Matrix(rw)->clear timezone
```


Downloaded from www.Manualslib.com manuals search engine

14

Node Alias Configuration

This chapter describes node alias commands and how to use them.

Configuring Node Aliases

Purpose

To review, configure, disable and re-enable node (port) alias functionality, which determines what network protocols are running on one or more ports.

Commands

For information about...	Refer to page...
show nodealias	14-1
show nodealias mac	14-2
show nodealias protocol	14-4
show nodealias config	14-5
set nodealias	14-6
set nodealias maxentries	14-7
clear nodealias	14-7
clear nodealias config	14-8

show nodealias

Use this command to display node alias properties for one or more ports.

Syntax

show nodealias [*port-string*]

Parameters

port-string	(Optional) Displays node alias properties for specific port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.

Downloaded from www.Manualslib.com manuals search engine

Defaults

If *port-string* is not specified, node alias properties will be displayed for all ports.

Mode

Switch command, Read-Only.

Usage

Node aliases are dynamically assigned upon packet reception to ports enabled with an alias agent, which is the default setting on Enterasys Matrix Series devices. Node aliases cannot be statically created, but can be deleted using the **clear node alias** command ("clear nodealias" on page 14-7).

Example

This example (a portion of the command output) shows how to display node alias properties for ge.3.12:

```
Matrix(rw)->show nodealias ge.3.12

Alias ID      = 1533917044        Active      = true
Vlan ID       = 1                 MAC Address = 00-e0-63-04-7b-00
Protocol      = ip                Source IP = 63.214.44.63
```

Table 14-1 provides an explanation of the command output.

Table 14-1 show nodealias Output Details

Output...	What it displays...
Alias ID	Alias dynamically assigned to this port.
Active	Whether or not this node alias entry is active.
Vlan ID	VLAN ID associated with this alias.
MAC Address	MAC address associated with this alias.
Protocol	Networking protocol running on this port.
Address / Source IP	When applicable, a protocol-specific address associated with this alias.

show nodealias mac

Use this command to display node alias entries based on MAC address and protocol.

Syntax

show nodealias mac *mac_address* [**ip** | **apl** | **mac** | **hsrp** | **dhcps** | **dhcpc** | **bootps** | **bootpc** | **ospf** | **vrrp** | **ipx** | **xrip** | **xsap** | **ipx20** | **rtmp** | **netBios** | **nbt** | **bgp** | **rip** | **igrp** | **dec** | **bpdu** | **udp**] [*port-string*]

Downloaded from www.Manualslib.com manuals search engine

Parameters

mac_address	Specifies a MAC address for which to display node alias entries. This can be a full or partial address.
ip | **apl** | **mac** | **hsrp** | **dhcps** | **dhcpc** | **bootps** | **bootpc** | **ospf** | **vrrp** | **ipx** | **xrip** | **xsap** | **ipx20** | **rtmp** | **netBios** | **nbt** | **bgp** | **rip** | **igrp** | **dec** | **bpdu** | **udp**	(Optional) Displays node alias entries for one of the following protocols: • Internet Protocol • Appletalk • Media Access Control • Hot Standby Routing Protocol • Dynamic Host Control Protocol Server • Dynamic Host Control Protocol Client • Boot Protocol Server • Boot Protocol Client • Open Shortest Path First • Virtual Router Redundancy Protocol • Internet Packet Exchange • IPX Routing Information Protocol • IPX Service Access Point • PX Protocol 20 packet • Routing Table Maintenance Protocol • NetBIOS (raw) • NetBIOS (over TCP/IP) • Border Gateway Protocol • Routing Information Protocol • Interior Gateway Routing Protocol • Digital Equipment Corporation • Bridge Protocol Data Unit • User Datagram Protocol
port-string	(Optional) Displays node alias properties for specific port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.

Defaults

- If protocol is not specified, node alias entries for all protocols will be displayed.
- If *port-string* is not specified, node alias entries will be displayed for all ports.

Mode

Switch command, Read-Only.

Downloaded from www.Manualslib.com manuals search engine

Example

This example shows how to display node alias entries for BPDU traffic on MAC addresses beginning with 00-e0. Refer back to Table 14-1 for a description of the command output.

```
Matrix(rw)->show nodealias mac 00-e0 bpdu
Port: lag.0.1   Time: 0 days 01 hrs 34 mins 53 secs
-------------------------------------------------------
Alias ID         = 306783575       Active           = true
Vlan ID          = 1               MAC Address      = 00-e0-63-59-f4-3d
Protocol         = bpdu

Port: lag.0.1   Time: 0 days 01 hrs 34 mins 54 secs
-------------------------------------------------------
Alias ID         = 306783579       Active           = true
Vlan ID          = 1               MAC Address      = 00-e0-63-59-f4-55
Protocol         = bpdu

Port: ge.3.14   Time: 0 days 00 hrs 00 mins 46 secs
-------------------------------------------------------
Alias ID         = 613566759       Active           = true
Vlan ID          = 1               MAC Address      = 00-e0-63-97-4b-69
Protocol         = bpdu

Port: ge.3.17   Time: 0 days 03 hrs 03 mins 52 secs
-------------------------------------------------------
Alias ID         = 613566837       Active           = true
Vlan ID          = 1               MAC Address      = 00-e0-63-97-d0-a0
Protocol         = bpdu
```

show nodealias protocol

Use this command to display node alias entries based on protocol and protocol address.

Syntax

show nodealias protocol {**ip** | **apl** | **mac** | **hsrp** | **dhcps** | **dhcpc** | **bootps** | **bootpc** | **ospf** | **vrrp** | **ipx** | **xrip** | **xsap** | **ipx20** | **rtmp** | **netBios** | **nbt** | **bgp** | **rip** | **igrp** | **dec** | **bpdu** | **udp**} [**ip-address** *ip-address*] [*port-string*]

Downloaded from www.Manualslib.com manuals search engine

Parameters

ip | **apl** | **mac** | **hsrp** | **dhcps** | **dhcpc** | **bootps** | **bootpc** | **ospf** | **vrrp** | **ipx** | **xrip** | **xsap** | **ipx20** | **rtmp** | **netBios** | **nbt** | **bgp** | **rip** | **igrp** | **dec** | **bpdu** | **udp**	Specifies the protocol for which to display node alias entries. Refer back **show nodealias mac** ("show nodealias mac" on page 14-2) for a detailed description of these parameters.
ip-address *ip-address*	(Optional) Used for IP protocol only, displays node alias entries for a specific source address.
port-string	(Optional) Displays node alias entries for specific port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.

Defaults

- If *ip-address* is not specified for the IP protocol, IP-related entries will be displayed from all source addresses.
- If *port-string* is not specified, node alias entries will be displayed for all ports.

Mode

Switch command, Read-Only.

Example

This example shows how to display node alias entries for IP traffic on ge.3.16. Refer back to Table 14-1 for a description of the command output.

```
Matrix(rw)->show nodealias protocol ip ge.3.16
Port: ge.3.16 Time: 1 days 03 hrs 33 mins 47 secs
-----------------------------------------------------------
Alias ID          = 1533917141      Active          = true
Vlan ID           = 1               MAC Address     = 00-e0-63-04-7b-00
Protocol          = ip              Source IP       = 199.45.62.25
```

show nodealias config

Use this command to display node alias configuration settings on one or more ports.

Syntax

show nodealias config [*port-string*]

Parameters

port-string	(Optional) Displays node alias configuration settings for specific port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.

Downloaded from www.Manualslib.com manuals search engine

Defaults

If *port-string* is not specified, node alias configurations will be displayed for all ports.

Mode

Switch command, Read-Only.

Example

This example shows how to display node alias configuration settings for ports fe.2.1 through 9:

```
Matrix(rw)->show nodealias config fe.2.1-9
Port Number        Max Entries         Used Entries         Status
-----------        -----------         ------------         ------
fe.2.1             16                  0                    Enabled
fe.2.2             47                  0                    Enabled
fe.2.3             47                  2                    Enabled
fe.2.4             47                  0                    Enabled
fe.2.5             47                  0                    Enabled
fe.2.6             47                  2                    Enabled
fe.2.7             47                  0                    Enabled
fe.2.8             47                  0                    Enabled
fe.2.9             4000                1                    Enabled
```

Table 14-2 provides an explanation of the command output.

Table 14-2 show nodealias config Output Details

Output...	What it displays...
Port Number	Port designation.
Max Entries	Maximum number of alias entries configured for this port. Set using the **set nodealias maxentries** command (“set nodealias maxentries” on page 14-7).
Used Entries	Number of alias entries (out of the maximum amount configured) already used by this port.
Status	Whether or not a node alias agent is enabled (default) or disabled on this port.

set nodealias

Use this command to enable or disable a node alias agent on one or more ports.

Syntax

set nodealias {**enable** | **disable**} *port-string*

Parameters

enable | **disable**	Enables or disables a node alias agent.
port-string	Specifies the port(s) on which to enable or disable a node alias agent. For a detailed description of possible *port-string* values, refer to “Port String Syntax Used in the CLI” on page 4-2.

Downloaded from www.Manualslib.com manuals search engine

Defaults

None.

Mode

Switch command, Read-Write.

Usage

Upon packet reception, node aliases are dynamically assigned to ports enabled with an alias agent, which is the default setting on Enterasys Matrix Series devices. Node aliases cannot be statically created, but can be deleted using the clear node alias command as described in "clear nodealias" on page 14-7.

Example

This example shows how to disable the node alias agent on fe.1.3:

```
Matrix(rw)->set nodealias disable fe.1.3
```

set nodealias maxentries

Use this command to set the maximum number of node alias entries allowed for one or more ports.

Syntax

set nodealias maxentries *val port-string*

Parameters

val	Specifies the maximum number of alias entries.
port-string	Specifies the port(s) on which to set the maximum entry value. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to set the maximum node alias entries to 1000 on fe.1.3:

```
Matrix(rw)->set nodealias maxentries 1000 fe.1.3
```

clear nodealias

Use this command to remove one or more node alias entries.

Syntax

clear nodealias {**port-string** *port-string* | **alias-id** *alias-id*}

Downloaded from www.Manualslib.com manuals search engine

Parameters

port-string *port-string*	Specifies the port(s) on which to remove all node alias entries. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.
alias-id *alias-id*	Specifies the ID of the node alias to remove. This value can be viewed using the **show nodealias** command as described in "show nodealias" on page 14-1.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to clear all node alias entries on fe.1.3:

```
Matrix(rw)->clear nodealias port-string fe.1.3
```

clear nodealias config

Use this command to reset node alias state to enabled and clear the maximum entries value.

Syntax

clear nodealias config *port-string*

Parameters

port-string	Specifies the port(s) on which to reset the node alias configuration. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to reset the node alias configuration on fe.1.3:

```
Matrix(rw)->clear nodealias config fe.1.3
```


Downloaded from www.Manualslib.com manuals search engine

15

NetFlow Configuration

This chapter describes NetFlow commands and how to use them.

Note: An Enterasys Feature Guide document that contains a complete discussion on NetFlow configuration exists at the following Enterasys web site: http://www.enterasys.com/support/manuals/

Configuring NetFlow

NetFlow is a protocol developed for collecting IP traffic information. Network devices (switches and routers) with NetFlow enabled generate NetFlow flow records, which are exported from the device in UDP packets and collected by a NetFlow collector.

Enterasys Matrix DFE Implementation

The Enterasys Matrix DFE flow-based architecture provides a powerful mechanism for collecting network flow statistics, with reporting capacity that scales with the addition of each DFE blade. For each flow, packet and byte count statistics are collect by the DFE forwarding hardware. The flow report generation logic is distributed, permitting each blade to report flows on its own ports.

The Enterasys Matrix DFE implementation enables the collection of NetFlow data on both switched and routed frames, allowing DFE blades in all areas of a network infrastructure to collect and report flow data. Routing does not need to be enabled to utilize NetFlow data collection. Flow detail depends on the content of the frame and the path the frame takes through the switch.

Operation

NetFlow can be enabled on all ports on a Enterasys Matrix system, including fixed front panel ports, LAG ports, NEM ports, and FTM1 backplane ports. Router interfaces which map to VLANs may not be enabled directly.

NetFlow records are generated only for flows for which a hardware connection has been established. As long as the network connection exists (and NetFlow is enabled), NetFlow records will be generated. Flows that are switched in firmware (soft forwarded) will not have NetFlow records reported. For flows that are routed, the DFE firmware reports the source and destination ifIndexes as the physical ports, not routed interfaces.

In the case of a LAG port, the blade(s) that the physical ports are on will generate NetFlow records independently. They will however, report the source ifIndex as the LAG port. The Flow Sequence Counter field in the NetFlow Header is unique per blade. The Engine ID field of the NetFlow Header is used to identify each unique blade. Each blade functions as a separate Netflow engine.

When NetFlow is enabled, each DFE blade in the Enterasys Matrix system will transmit a NetFlow packet when:

Downloaded from www.Manualslib.com manuals search engine

- It has accumulated the maximum number of NetFlow records per packet, which is 30, or
- It has accumulated fewer than 30 NetFlow records and the active flow timer has expired, or
- The flow expires (ages out or is invalidated).



Note: A flow is a unidirectional sequence of packets having a set of common properties, travelling between between a source and a destination endpoint. A flow is created on the Enterasys Matrix device when the MAC destination address of a packet is learned on a port and torn down when either it ages out or it is explicitly torn down by the firmware.

Version Support

The Enterasys Matrix DFE firmware supports NetFlow Version 5 and Version 9. For more information about Version 9 data export format, refer to RFC 3954, "Cisco Systems NetFlow Services Export Version 9."

When transmitting NetFlow Version 5 reports, the DFE blade uses "netflow interface" indexes. Normally these would be actual MIB-2 ifIndex values, but the Version 5 record format limits the values to 2 bytes, which is not sufficient to hold 4 byte ifIndexes. NetFlow collector applications that use the in/out interface indexes to gather SNMP data about the interface (such as ifName) must translate the interface indexes using the Enterasys MIB etsysNetflowMIB (1.3.1.6.1.4.1.5624.1.2.61).

NetFlow Version 9 records generated by DFE blades use true MIB-2 ifIndex values since the template mechanism permits transmission of 4 byte ifIndexes. Version 9 also uses 8 byte packet and byte counters, so they are less likely to roll over. Check with your collector provider to determine if they provide the necessary support.

The current Version 9 implementation:

- Does not support aggregation caches
- Provides 4 predefined templates. The appropriate template is selected for each flow depending on whether the flow is routed or switched, and whether it is a TCP/UDP packet or not.

Version 9 templates are re-transmitted when:

- The timeout is reached. The default is 30 minutes but is user configurable using the **set netflow template timeout** command ("set netflow template" on page 15-9).

Templates are sent from every blade when the timeout is reached.

- The packet refresh rate is reached. The default is every 20 packets, but is user configurable using the **set netflow template refresh-rate** command ("set netflow template" on page 15-9).

Templates are sent as a result of the refresh rate by each blade, since each blade handles it's own packet transmission. For flow generation and processing efficiency reasons, Enterasys recommends that customers configure their Enterasys Matrix systems so that templates are not generated more often than once per second, as a minimum. For more information about setting the refresh rate, see the Usage discussion in "set netflow template" on page 15-9.

Commands

For information about...	Refer to page...
show netflow	15-3
set netflow cache	15-4

Downloaded from www.Manualslib.com manuals search engine

For information about...	Refer to page...
clear netflow cache	15-4
set netflow export-destination	15-5
clear netflow export-destination	15-5
set netflow export-interval	15-6
clear netflow export-interval	15-7
set netflow port	15-7
clear netflow port	15-8
set netflow export-version	15-8
clear netflow export-version	15-9
set netflow template	15-9
clear netflow template	15-11

show netflow

Use this command to display NetFlow configuration information and/or statistics.

Syntax

show netflow [**config** [*port-string*]] [**statistics** [**export**]]

Parameters

config	(Optional) Show the NetFlow configuration.
statistics	(Optional) Show the NetFlow statistics.
export	(Optional) Show the NetFlow export statistics.
port-string	Specifies the port or ports to display.

Defaults

If **config** is entered by no *port-string*, information for all ports is displayed.

If **statistics** is entered but not **export**, all statistics are displayed.

Mode

Switch command, Read Only.

Example

This example shows how to display both Netflow configuration information and statistics:

```
Matrix(rw)->show netflow

Cache Status:          enabled
Destination IP:        10.10.1.1
Destination UDP Port:  2055
Export Version:        5
```


Downloaded from www.Manualslib.com manuals search engine

```
Export Interval:       30 (min)
Number of Entries:     196607
Inactive Timer:        40 (sec)
Template Refresh-rate: 20 (packets)
Template Timeout:      30 (min)

Enabled Ports:
----------------
ge.1.11,23
```

set netflow cache

Use this command to enable (create) or disable (free up) a NetFlow cache on each DFE blade in the Enterasys Matrix system.

Syntax

set netflow cache {**enable** | **disable**}

Parameters

enable | **disable**	Enable or disable the NetFlow cache.

Defaults

None.

Mode

Switch command, Read-Write.

Usage

A NetFlow cache maintains NetFlow information for all active flows. By default, NetFlow caches are not created.

Example

This example shows how to enable, or create, a NetFlow cache on each DFE blade in the system:

```
Matrix(rw)->set netflow cache enable
```

clear netflow cache

Use this command to remove, or free up, the NetFlow caches on each DFE blade in the Enterasys Matrix system.

Syntax

clear netflow cache

Parameters

None.

Downloaded from www.Manualslib.com manuals search engine

Defaults

None.

Mode

Switch command, Read-Write.

Usage

When this command is executed, NetFlow is effectively disabled on the system.

Example

This example shows how to remove the NetFlow caches on the DFE blades and disable NetFlow:

```
Matrix(rw)->clear netflow cache
```

set netflow export-destination

Use this command to configure the NetFlow collector destination.

Syntax

set netflow export-destination *ip-address* [*udp-port*]

Parameters

ip-address	Specifies the IP address of the NetFlow collector.
udp-port	(Optional) Specifies the UDP port number used by the NetFlow collector. Default is 2055.

Defaults

None.

Mode

Switch command, Read-Write.

Usage

By default, no collector address is configured. Only one collector destination per Enterasys Matrix system can be configured.

Example

This example shows how to set the IP address of the NetFlow collector:

```
Matrix(rw)->set netflow export-destination 10.10.1.1
```

clear netflow export-destination

Use this command to clear the NetFlow collector IP address.

Syntax

clear netflow export-destination [*ip-address* [*udp-port*]]

Downloaded from www.Manualslib.com manuals search engine

Parameters

ip-address	(Optional) Specifies the IP address of the NetFlow collector to clear.
udp-port	(Optional) Specifies the UDP port number used by NetFlow collector.

Defaults

Since only one collector address per Enterasys Matrix system is supported, entering the IP address and UDP port information is not required. Executing this command without any parameters will return the collector address to "Not Configured."

Mode

Switch command, Read-Write.

Example

This example shows how to clear the NetFlow collector address:

```
Matrix(rw)->clear netflow export-destination
```

set netflow export-interval

Use this command to configure the NetFlow export interval.

Syntax

set netflow export-interval *interval*

Parameters

interval	Set the active flow timer value, between 1 to 60 minutes. The default value is 30 minutes.

Defaults

None.

Mode

Switch command, Read-Write.

Usage

Each DFE blade in the Enterasys Matrix system will transmit a NetFlow packet when:

- It has accumulated the maximum number of NetFlow records per packet, which is 30, or
- It has accumulated fewer than 30 NetFlow records and the active flow timer has expired, or
- The flow expires (ages out or is invalidated).

Example

This example shows how to set the NetFlow export interval to 10 minutes:

```
Matrix(rw)->set netflow export-interval 10
```


Downloaded from www.Manualslib.com manuals search engine

clear netflow export-interval

Use this command to clear NetFlow export interval to its default of 30 minutes.

Syntax

clear netflow export-interval

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to return the NetFlow export interval to its default value:

```
Matrix(rw)->clear netflow export-interval
```

set netflow port

Use this command to enable NetFlow collection on a port.

Syntax

set netflow port *port-string* {**enable** | **disable**}

Parameters

port-string	Specifies the port or ports on which to enable or disable NetFlow collection.
enable | **disable**	Enables or disables NetFlow collection.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to enable NetFlow collection on port ge.1.1:

```
Matrix(rw)->set netflow port ge.1.1 enable
```


Downloaded from www.Manualslib.com manuals search engine

clear netflow port

Use this command to return a port to the default NetFlow collection state of disabled.

Syntax

clear netflow port *port-string*

Parameters

port-string	Specifies the port or ports on which to disable NetFlow collection.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to disable NetFlow collection on port ge.1.1:

```
Matrix(rw)->clear netflow port ge.1.1
```

set netflow export-version

Use this command to set the NetFlow flow record format used to export data.

Syntax

set netflow export-version {**5** | **9**}

Parameters

5 | **9**	Specifies the NetFlow flow record format to use when exporting NetFlow packets, either Version 5 or 9. The default is Version 5.

Defaults

None.

Mode

Switch command, Read-Write.

Usage

Refer to "Version Support" on page 15-2 for more information about NetFlow version support. Use the **show netflow config** command ("show netflow" on page 15-3) to display the current NetFlow version.

Downloaded from www.Manualslib.com manuals search engine

Example

This example shows how to set the flow record format to Version 9:

```
Matrix(rw)->set netflow export-version 9
```

clear netflow export-version

Use this command to return the NetFlow flow record format used to export data to the default of Version 5.

Syntax

clear netflow export-version

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Write.

Usage

Use the **show netflow config** command ("show netflow" on page 15-3) to display the current NetFlow version.

Example

This example shows how to return the flow record format to Version 5:

```
Matrix(rw)->clear netflow export-version
```

set netflow template

Use this command to configure the NetFlow Version 9 template refresh rate and/or timeout values.

Syntax

set netflow template {[**refresh-rate** *packets*] [**timeout** *minutes*]}

Downloaded from www.Manualslib.com manuals search engine

Parameters

refresh-rate *packets*	The number of export packets sent that causes a template to be retransmitted by an individual DFE blade. The value of *packets* can range from 1 to 600. The default value is 20 packets.
timeout *minutes*	The length of the timeout period, in minutes, after which a template is retransmitted by all blades in the system. The value of *minutes* can range from 1 to 3600. The default value is 30 minutes.

Defaults

At least one of the **refresh-rate** or **timeout** parameters must be specified, although both can be specified on one command line.

Mode

Switch command, Read-Write.

Usage

Version 9 template records have a limited lifetime and must be periodically refreshed. Templates are retransmitted when either:

- The packet refresh rate is reached, or
- The template timeout is reached.

Template refresh based on the timeout period is performed on every blade. Since each DFE blade handles its own packet transmissions, template refresh based on number of export packets sent is managed by each blade independently.

The refresh rate defines the maximum delay a new or restarted NetFlow collector would experience until it learns the format of the data records being forwarded (from the template referenced by the data records). Refresh rates affect NetFlow collectors during their start up when they must ignore incoming data flow reports until the required template is received.

Setting the appropriate refresh rate for your Enterasys Matrix system must be determined, since the default settings of a 20 packet refresh rate and a 30 minute timeout may not be optimal for your environment. For example, a switch processing an extremely slow flow rate of, say, 20 packets per half hour, would refresh the templates only every half hour using the default settings, while a switch sending 300 flow report packets per second would refresh the templates 15 times per second.

Enterasys recommends that you configure your Enterasys Matrix system so it does not refresh templates more often than once per second.

Use the **show netflow config** command (“show netflow” on page 15-3) to display the currently configured values.

Example

This example shows how to set the Version 9 template packet refresh rate to 50 packets and the timeout value to 45 minutes:

```
Matrix(rw)->set netflow template refresh-rate 50 timeout 45
```


Downloaded from www.Manualslib.com manuals search engine

clear netflow template

Use this command to reset the Version 9 template refresh rate and/or timeout values to their default values.

Syntax

```
clear netflow template {[refresh-rate] [timeout]}
```

Parameters

refresh-rate	Clear the template packet refresh rate to the default value of 20 packets.
timeout	Clear the template timeout to the default value of 30 minutes.

Defaults

At least one of the **refresh-rate** or **timeout** parameters must be specified, although both can be specified on one command line.

Mode

Switch command, Read-Write.

Example

This example shows how to return the Version 9 template packet refresh rate to 20 packets and the timeout value to 30 minutes:

```
Matrix(rw)->set netflow template refresh-rate 50 timeout 30
```


Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

16

IP Configuration

This chapter describes the Internet Protocol (IP) configuration set of commands and how to use them.



Router: Unless otherwise noted, the commands covered in this chapter can be executed only when the device is in router mode. For details on how to enable router configuration modes, refer to "Enabling Router Configuration Modes" on page 2-103.

For information about...	Refer to page...
Configuring Routing Interface Settings	16-1
Managing Router Configuration Files	16-8
Performing a Basic Router Configuration	16-11
Reviewing and Configuring the ARP Table	16-12
Configuring Broadcast Settings	16-19
Reviewing IP Traffic and Configuring Routes	16-22
Configuring Debug IP Packet	16-30

Configuring Routing Interface Settings

About Loopback Versus VLAN Interfaces

Loopback interfaces are different from VLAN routing interfaces because they allow you to disconnect the operation of routing protocols from network hardware operation, improving the reliability of IP connections. A loopback interface is always reachable. The IP address assigned to the loopback interface is used as the router ID, which helps when running protocols like OSPF, because OSPF can be running even when the outbound interface is down. IP packets routed to the loopback interface are rerouted back to the router or access server and processed locally.

Routing interface configuration commands in this guide will configure either a VLAN or loopback interface, depending on your choice of parameters, as shown in Table 16-1.

Downloaded from www.Manualslib.com manuals search engine

Table 16-1 VLAN and Loopback Interface Configuration Modes

For Routing Interface Type...	Enter (in Global Configuration Mode)...	Resulting Prompt...
VLAN	**vlan** *vlan-id*	**Matrix>Router (config-if(Vlan 1))#**
Loopback	**loopback** *loopback-id*	**Matrix>Router (config-if (Lpbk 1))#**
Local (software loopback)	**lo** *local-id*	**Matrix>Router (config-if (Lo 1))#**

For details on how to enable all router CLI configuration modes, refer back to Table 2-9.

For details on configuring routing protocols, refer to Chapter 21.

Purpose

To enable routing interface configuration mode on the device, to create VLAN or loopback routing interfaces, to review the usability status of interfaces configured for IP, to set IP addresses for interfaces, and to enable interfaces for IP routing at device startup.

Commands

For information about...	Refer to page...
show interface	16-2
interface	16-3
ip ecm-forwarding-algorithm	16-4
show ip interface	16-5
ip address	16-6
no shutdown	16-7

show interface

Use this command to display information about one or more interfaces (VLANs or loopbacks) configured on the router.

Syntax

show interface [**vlan** *vlan-id* | **loopback** *loopback-id* | **lo** *local-id*]

Parameters

vlan *vlan-id* | **loopback** *loopback-id* | **lo** *local-id*	(Optional) Displays interface information for a specific VLAN, loopback, or local interface. This interface must be configured for IP routing as described in "Pre-Routing Configuration Tasks" on page 2-100.

Defaults

If interface type is not specified, information for all routing interfaces will be displayed.

Downloaded from www.Manualslib.com manuals search engine

Mode

Router command, Any router mode.

Example

This example shows how to display information for all interfaces configured on the router. In this case, one loopback interface has been configured for routing. For a detailed description of this output, refer to Table 16-2Matrix>Router#show interface :

```
Vlan 1 is Administratively DOWN
 Vlan 1 is Operationally DOWN
 Mac Address is: 0001.f4da.2cba
 The name of this device is Vlan 1
 The MTU is 1500 bytes
 The bandwidth is 10000 Mb/s
 Encapsulation ARPA, Loopback not set
 ARP type: ARPA, ARP Timeout: 14400 seconds

lo is Administratively UP
 lo is Operationally UP
 Internet Address is 127.0.0.1, Subnet Mask is 255.255.255.0
 The name of this device is lo
 The MTU is 1500 bytes
 The bandwidth is 10000 Mb/s
```

interface

Use this command to configure interfaces for IP routing.

Syntax

interface {**vlan** *vlan-id* | **loopback** *loopback-id*}

Parameters

vlan *vlan-id* | **loopback** *loopback-id*	Specifies the number of the VLAN or loopback interface to be configured for routing. This interface must be configured for IP routing as described in "Pre-Routing Configuration Tasks" on page 2-100.

Defaults

None.

Mode

Router command, Global configuration mode: **Matrix>Router(config)#**

Usage

This command enables interface configuration mode from global configuration mode, and, if the interface has not previously been created, this command creates a new routing interface. For

Downloaded from www.Manualslib.com manuals search engine

details on configuration modes supported by the Enterasys Matrix Series device and their uses, refer to Table 2-9 in "Enabling Router Configuration Modes" on page 2-103.

VLANs must be created from the switch CLI before they can be configured for IP routing. For details on creating VLANs and configuring them for IP, refer to "Reviewing and Configuring Routing" on page 2-101.

Each VLAN or loopback interface must be configured for routing separately using the **interface** command. To end configuration on one interface before configuring another, type **exit** at the command prompt. Enabling interface configuration mode is required for completing interface-specific configuration tasks. For an example of how these commands are used, refer to Figure 2-8 in "Pre-Routing Configuration Tasks" on page 2-100.

Each Enterasys Matrix Series routing module or standalone device can support up to 96 routing interfaces. Each interface can be configured for the RIP and/or OSPF routing protocols.

Example

This example shows how to enter configuration mode for VLAN 1:

```
Matrix>Router#configure terminal
Matrix>Router(config)#interface vlan 1
Matrix>Router(config-if(Vlan 1))#
```

ip ecm-forwarding-algorithm

Use this command to enable ECM (Equal Cost Multipath) for forwarding IP packets on routing interfaces.

Syntax

ip ecm-forwarding-algorithm [**hash-thold** | **round-robin**]

no ip ecm-forwarding-algorithm

Parameters

hash-thold | **round-robin**	(Optional) Sets the ECM forwarding algorithm as hash threshold or round-robin.

Defaults

If algorithm is not specified, hash threshold will be set.

Mode

Router command, Global configuration: **Matrix>Router(config)#**

Usage

The "no" form of this command disables ECM mode.

Example

This example shows how to enable ECM mode:

```
Matrix>Router(config)#ip ecm-forwarding-algorithm
```


Downloaded from www.Manualslib.com manuals search engine

show ip interface

Use this command to display information, including administrative status, IP address, MTU (Maximum Transmission Unit) size and bandwidth, and ACL configurations, for interfaces configured for IP.

Syntax

show ip interface [**vlan** *vlan-id* | **loopback** *loopback-id* | **lo** *loopback-id*]

Parameters

vlan *vlan-id* | **loopback** *loopback-id* **lo** *loopback-id*	(Optional) Displays information for a specific VLAN, loopback, or local interface. This interface must be configured for IP routing as described in "Pre-Routing Configuration Tasks" on page 2-100.

Defaults

If interface type is not specified, status information for all routing interfaces will be displayed.

Mode

Router command, Any router mode.

Example

This example shows how to display configuration information for VLAN 1: Matrix>Router#show ip interface vlan 1

```
Vlan 1 is Oper DOWN
Frame Type ARPA
MAC-Address 0001.f4da.2cba
Incoming Access List is not Set
Outgoing Access List is not Set
IP Helper Address is not Set
MTU is 1500 bytes
ARP Timeout is 14400 seconds
Proxy Arp is Enabled
Gratuitous arp learning is not set
ICMP Re-Directs are enabled
ICMP Unreachables are always sent
ICMP Mask Replies are always sent
Policy routing disabled
```

Table 16-2 provides an explanation of the command output.

Table 16-2 show ip interface Output Details

Output...	What it displays...
Vlan | Lpbk | Lo *N*	Whether the interface is administratively and operationally up or down.
IP Address	Interface's IP address and mask. Set using the **ip address** command as described in "ip address" on page 16-6.
Frame Type	Encapsulation type used by this interface. Set using the **arp** command as described in "arp" on page 16-14.

Downloaded from www.Manualslib.com manuals search engine

Table 16-2 show ip interface Output Details (continued)

Output...	What it displays...
MAC-Address	MAC address mapped to this interface. Set using the **ip mac-address** command as described in "ip mac-address" on page 16-17.
Incoming | Outgoing Access List	Whether or not an access control list (ACL) has been configured on this interface using the commands described in "Configuring Access Lists" on page 24-15.
IP Helper Address	Whether or not an IP address has been designated for forwarding UDP datagrams from this interface. Set using the **ip helper-address** command as described in "ip helper-address" on page 16-21
MTU	Interface's Maximum Transmission Unit size.
ARP Timeout	Duration for entries to stay in the ARP table before expiring. Set using the **arp timeout** command as described in "arp timeout" on page 16-17.
Proxy Arp	Whether or not proxy ARP is enabled or disabled for this interface. Set using the **ip proxy arp** command as described in "ip proxy-arp" on page 16-16.
ICMP	ICMP (ping) settings. By default, ICMP messaging is enabled on a routing interface for both echo-reply and mask-reply modes. If, for security reasons, ICMP has been disabled, it can be re-enabled using the **ip icmp** command as described in "ip icmp" on page 16-27.
Policy routing	Whether or not policy-based routing has been configured on this interface as described in "Configuring Denial of Service (DoS) Prevention" on page 24-22.

ip address

Use this command to set, remove, or disable a primary or secondary IP address for an interface.

Syntax

ip address *ip-address ip-mask* [**secondary**]

no ip address *ip-address ip-mask*

Parameters

ip-address	Specifies the IP address of the interface to be added or removed.
ip-mask	Specifies the mask for the associated IP subnet.
secondary	(Optional) Specifies that the configured IP address is a secondary address.

Defaults

If **secondary** is not specified, the configured address will be the primary address for the interface.

Mode

Router command, Interface configuration: **Matrix>Router(config-if(Vlan 1))#**

Downloaded from www.Manualslib.com manuals search engine

Usage

Each Enterasys Matrix Series routing module or standalone device supports up to 96 routing interfaces, with up to 50 secondary addresses (200 maximum per router) allowed for each primary IP address.

The “no” form of this command removes the specified IP address and disables the interface for IP processing.

Example

This example sets the IP address to 192.168.1.1 and the network mask to 255.255.255.0 for VLAN 1:

```
Matrix>Router(config)#interface vlan 1
Matrix>Router(config-if(Vlan 1))#ip address 192.168.1.1 255.255.255.0
```

no shutdown

Use this command to enable an interface for IP routing and to allow the interface to automatically be enabled at device startup.

Syntax

no shutdown

Parameters

None.

Defaults

None.

Mode

Router command, Interface configuration: **Matrix>Router(config-if(Vlan 1))#**

Usage

The **shutdown** form of this command disables an interface for IP routing.

Example

This example shows how to enable VLAN 1 for IP routing:

```
Matrix>Router(config)#interface vlan 1
Matrix>Router(config-if(Vlan 1))#no shutdown
```


Downloaded from www.Manualslib.com manuals search engine

Managing Router Configuration Files

Each Enterasys Matrix Series device provides a single configuration interface which allows you to perform both switch and router configuration with the same command set. When a redundancy license is available and has been activated, the device also provides redundant, distributed copies of each router configuration in the event that DFE modules are added or removed from the Enterasys Matrix chassis. This section demonstrates managing configuration files while operating in router mode only. For a sample of how to use these commands interchangeably with the Enterasys Matrix Series single configuration interface commands, refer to "Performing a Basic Router Configuration" on page 16-11.

Purpose

To review and save the current router configuration, and to disable IP routing.

Commands

For information about...	Refer to page...
show running-config	16-8
write	16-9
no ip routing	16-10

show running-config

Use this command to display the non-default, user-supplied commands entered while configuring the device.

Syntax

show running-config

Parameters

None.

Defaults

None.

Mode

Router command, Any router mode.

Example

This example shows how to display the current router operating configuration:

```
Matrix>Router#show running-config
!
router id 192.168.100.1
!
 interface loopback 1
```


Downloaded from www.Manualslib.com manuals search engine

```
  ip address 192.168.100.1 255.255.255.255
  no shutdown
!
 interface vlan 10
  ip address 99.99.2.10 255.255.255.0
  no shutdown
!
 router ospf 1
  network 99.99.2.0     0.0.0.255 area 0.0.0.0
network 192.168.100.1 0.0.0.0   area 0.0.0.0
```

write

Use this command to save or delete the router running configuration, or to display it to output devices.

Syntax

write [**erase** | **file** [**filename** *config-file*] | **terminal**]

Parameters

erase	(Optional) Deletes the router-specific file.
file	(Optional) Saves the router-specific configuration to NVRAM.
filename *config-file*	(Optional) Saves the router-specific configuration to a file.
terminal	(Optional) Displays the current router-specific configuration to the terminal session.

Defaults

If no parameters are specified, the running configuration will be displayed to the terminal session.

Mode

Router command, Privileged EXEC: **Matrix>Router#**

Usage

The **write file** command must be executed in order to save the router configuration to NVRAM. If this command is not executed, router configuration changes will not be saved upon reboot.

Example

This example shows how to display the router-specific configuration to the terminal:Matrix>Router#write terminal

```
Enable
Config t

interface vlan 1
 iP Address 182.127.63.1 255.255.255.0
 no shutdown
```


Downloaded from www.Manualslib.com manuals search engine

```
interface vlan 2
 iP Address 182.127.62.1 255.255.255.0
 no shutdown
exit

router rip
network 182.127.0.0
exit
disable
exit
```

no ip routing

Use this command to disable IP routing on the device and remove the routing configuration.

Syntax

`no ip routing`

Parameters

None.

Defaults

None.

Mode

Router command, Global configuration: **Matrix>Router(config)#**

Usage

By default, IP routing is enabled when interfaces are configured for it as described in "Configuring Routing Interface Settings" on page 16-1.

Example

This example shows how to disable IP routing on the device:

```
Matrix>Router(config)#no ip routing
```


Downloaded from www.Manualslib.com manuals search engine

Performing a Basic Router Configuration

Using Router-Only Config Files

Although the Enterasys Matrix Series' single configuration interface provides one set of commands to perform both switch and router configuration, it is still possible to use router-only commands to configure the router. To do so, you need to add router config wrappers to your existing router config files, as shown in Figure 16-1.

Figure 16-1 Example of a Simple Enterasys Matrix Series Router Config File

```
begin router

enable
conf t
write file
exit
disable
exit

end router
```

Displaying or Writing the Current Config to a File

The Enterasys Matrix Series' single configuration interface allows you use the **show config** command to display or write the current router configuration to a file. For details, refer to "show config" on page 2-85.

Configuring the Router

You can configure the router using either of the following methods.

Using a downloaded file...

1. Download a router config file to the standalone or chassis using the **copy** command as described in "copy" on page 2-86.
2. Run the **configure** command using the downloaded config file as described in "configure" on page 2-86.

Creating and saving a custom file...

1. Enable the router as described in "Enabling Router Configuration Modes" on page 2-103 and configure it manually. (Refer back to Figure 16-1 for an example of a basic config file.)
2. Save the configuration using the **write file** command as described in "write" on page 16-9.

Moving a Config File from Another Routing Module

To copy a router configuration from one module to another, proceed as follows:

1. From the routing module in which you wish to copy a config file, perform a **show config** on the file as described in "show config" on page 2-85.

Downloaded from www.Manualslib.com manuals search engine

2. Copy the config file to a place where it can be edited with a file editing program.
3. If you only want the router config, delete all the non-routing config elements and save the new file.
4. Change the routing instance to the module to which the config will be moved as described in "Enabling Router Configuration Modes" on page 2-103.
5. Use the **copy** command to move the config file to the new module as described in "copy" on page 2-86.
6. Run the **configure** command using the new config file as described in "configure" on page 2-86.

Reviewing and Configuring the ARP Table

Purpose

To review and configure the routing ARP table, to enable proxy ARP on an interface, and to set a MAC address on an interface.

Commands

For information about...	Refer to page...
show ip arp	16-12
arp	16-14
ip gratuitous-arp	16-15
ip gratuitous-arp-learning	16-15
ip proxy-arp	16-16
ip mac-address	16-17
arp timeout	16-17
clear arp-cache	16-18

show ip arp

Use this command to display entries in the ARP (Address Resolution Protocol) table. ARP converts an IP address into a physical address.

Syntax

show ip arp [*ip-address*] [**vlan** *vlan-id*] [*output-modifier*]

Downloaded from www.Manualslib.com manuals search engine

Parameters

ip-address	(Optional) Displays ARP entries related to a specific IP address.
vlan *vlan-id*	(Optional) Displays only ARP entries learned through a specific VLAN interface. This VLAN must be configured for IP routing as described in "Pre-Routing Configuration Tasks" on page 2-100.
output-modifier	(Optional) Displays ARP entries within a specific range. The syntax is to enter an "|" character, followed by a space, followed by a **begin**, **exclude**, or **include** keyword as follows: • | **begin** *ip-address* — Displays only ARP entries that begin with the specified IP address. • | **exclude** *ip-address* — Excludes ARP entries matching the specified IP address. • | **include** *ip-address* — Includes ARP entries matching the specified IP address.

Defaults

If no parameters are specified, all entries in the ARP cache will be displayed.

Mode

Any router mode.

Example

This example shows how to use the **show ip arp** command:

```
Matrix>Router#show ip arp
Protocol   Address           Age (min) Hardware Addr   Type      Interface
-------------------------------------------------------------------------------
Internet   134.141.235.251   0      0003.4712.7a99     ARPA      Vlan1
Internet   134.141.235.165   -      0002.1664.a5b3     ARPA      Vlan1
Internet   134.141.235.167   4      00d0.cf00.4b74     ARPA      Vlan2

Matrix>Router#show ip arp 134.141.235.165
Protocol   Address           Age (min) Hardware Addr   Type      Interface
-------------------------------------------------------------------------------
Internet   134.141.235.165   -      0002.1664.a5b3     ARPA      Vlan2

Matrix>Router#show ip arp vlan 2
Protocol   Address           Age (min) Hardware Addr   Type      Interface
-------------------------------------------------------------------------------
```

Internet 134.141.235.251 0 0003.4712.7a99 ARPA Vlan2

Table 16-3 provides an explanation of the command output.

Downloaded from www.Manualslib.com manuals search engine

Table 16-3 show ip arp Output Details

Output...	What it displays...
Protocol	ARP entry's type of network address.
Address	Network address mapped to the entry's MAC address.
Age (min)	Interval (in minutes) since the entry was entered in the table.
Hardware Addr	MAC address mapped to the entry's network address.
Type	Encapsulation type used for the entry's network address.
Interface	Interface (VLAN or loopback) through which the entry was learned.

arp

Use this command to add or remove permanent (static) ARP table entries.

Syntax

arp *ip-address mac-address* **arpa**

no arp *ip-address*

Parameters

ip-address	Specifies the IP address of a device on the network. Valid values are IP addresses in dotted decimal notation.
mac-address	Specifies the 48-bit hardware address corresponding to the *ip-address* expressed in hexadecimal notation.
arpa	Specifies ARPA as the type of ARP mapping.

Defaults

None.

Mode

Router command, Global configuration: **Matrix>Router(config)#**

Usage

Up to 1,000 static ARP entries are supported per Enterasys Matrix Series routing module or standalone device. A multicast MAC address can be used in a static ARP entry.

The "no" form of this command removes the specified permanent ARP entry.

Example

This example shows how to add a permanent ARP entry for the IP address 130.2.3.1 and MAC address 0003.4712.7a99:

```
Matrix>Router(config)#arp 130.2.3.1 0003.4712.7a99 arpa
```


Downloaded from www.Manualslib.com manuals search engine

ip gratuitous-arp

Use this command to override the normal ARP updating process, that occurs by default.

Syntax

ip gratuitous-arp {**ignore** | **reply** | **request**}

no ip gratuitous-arp

Parameters

ignore	Ignore all gratuitous ARP frames, no updates will occur. This option will also prevent any new learning from gratuitous arps, if the command **ip gratuitous-arp-learning** was used.("ip gratuitous-arp-learning" on page 16-15).
reply	Update from gratuitous arp reply only.
request	Update from gratuitous arp request only.

Defaults

None.

Mode

Router command, Interface configuration: **Matrix>Router(config-if(Vlan 1))#**

Usage

The "no" form of this command resumes default ARP processing as described in RFC 826, update an existing ARP entry from either a gratuitous ARP reply or request.

Example

This example shows how to enable ARP updating from gratuitous ARP requests on VLAN 1:

```
Matrix>Router(config)#interface vlan 1
Matrix>Router(config-if(Vlan 1))#ip gratuitous-arp request
```

ip gratuitous-arp-learning

Use this command to allow an interface to learn new ARP bindings using gratuitous ARP.

Syntax

ip gratuitous-arp-learning {**both** | **reply** | **request**}

no ip gratuitous-arp-learning

Parameters

both | **reply** | **request**	Allows learning from gratuitous ARP reply, ARP request, or from both the ARP reply and request.

Defaults

None.

Downloaded from www.Manualslib.com manuals search engine

Mode

Router command, Interface configuration: **Matrix>Router(config-if(Vlan 1))#**

Usage

This command will be in effect if the i**p gratuitous-arp ignore** command (“ip gratuitous-arp” on page 16-15) is used. There will be no learning from gratuitous ARP frames, even with the **ip gratuitous-arp-learning** command enabled.

The “no” form of this command disables gratuitous ARP learning.

Example

This example shows how to enable gratuitous ARP learning for both requests and replies on VLAN 1:

```
Matrix>Router(config)#interface vlan 1
Matrix>Router(config-if(Vlan 1))#ip gratuitous-arp-learning both
```

ip proxy-arp

Use this command to enable proxy ARP on an interface. This variation of the ARP protocol allows the routing module to send an ARP response on behalf of an end node to the requesting host.

Syntax

ip proxy-arp [**default-route**] [**local**]

no ip proxy-arp

Parameters

default-route	(Optional) Sets the router to respond to ARP requests for hosts that are only reachable via the default route. Typically, proxy arp is only used to reply to requests for host that are reachable via a non-default route.
local	(Optional) Allows the router to respond to ARP requests that are received on the interface to which this command is applied if the source IP address of the request is reachable on this interface.

Defaults

None.

Mode

Router command, Interface configuration: **Matrix>Router(config-if(Vlan 1))#**

Usage

Proxy ARP can lessen bandwidth use on slow-speed WAN links. It is enabled by default.

The “no” form of this command disables proxy ARP

Downloaded from www.Manualslib.com manuals search engine

Example

This example shows how to enable proxy ARPMatrix>Router(config)#interface vlan 1 on VLAN 1:

```
Matrix>Router(config-if(Vlan 1))#ip proxy-arp
```

ip mac-address

Use this command to set a MAC address on an interface.

Syntax

ip mac-address *address*

no ip mac-address

Parameters

address	Specifies a 48-bit MAC address in hexadecimal format.

Defaults

None.

Mode

Router command, Interface configuration: **Matrix>Router(config-if(Vlan 1))#**

Usage

By default, every routing interface uses the same MAC address. If the user needs interfaces to use different MAC addresses, this command will allow it. It is the user's responsibility to select a MAC address that will not conflict with other devices on the VLAN since the Enterasys Matrix Series device will not automatically detect this conflict.

The "no" form of this command clears the MAC address.

Example

This example shows how to set an IP MAC address of 000A.000A.000B. on VLAN 1:

```
Matrix>Router(config)#interface vlan 1
Matrix>Router(config-if(Vlan 1))#ip mac-address 000A.000A.000B
```

arp timeout

Use this command to set the duration (in seconds) for entries to stay in the ARP table before expiring.

Syntax

arp timeout *seconds*

no arp timeout *seconds*

Downloaded from www.Manualslib.com manuals search engine

Parameters

seconds	Specifies the time in seconds that an entry remains in the ARP cache. Valid values are **0** - **65535**. A value of 0 specifies that ARP entries will never be aged out.

Defaults

None.

Mode

Router command, Global configuration: **Matrix>Router(config)#**

Usage

The device can support up to 2000 outstanding unresolved ARP entries.

The "no" form of this command restores the default value of 14,400 seconds

Example

This example shows how to set the ARP timeout to 7200 seconds:

```
Matrix>Router(config)#arp timeout 7200
```

clear arp-cache

Use this command to delete all nonstatic (dynamic) entries from the ARP table.

Syntax

clear arp-cache

Parameters

None.

Defaults

None.

Mode

Privileged EXEC: **Matrix>Router#**

Example

This example shows how to delete all dynamic entries from the ARP table:

```
Matrix>Router#clear arp-cache
```


Downloaded from www.Manualslib.com manuals search engine

Configuring Broadcast Settings

Applying DHCP/BOOTP Relay

DHCP/BOOTP relay functionality is applied with the help of IP broadcast forwarding. A typical situation occurs when a host requests an IP address with no DHCP server located on that segment. A routing module can forward the DHCP request to a server located on another network if:

- IP forward-protocol is enabled for UDP as described in "ip forward-protocol" on page 16-20, and
- The address of the DHCP server is configured as a helper address on the receiving interface of the routing module forwarding the request, as described in "ip helper-address" on page 16-21.

The DHCP/BOOTP relay function will detect the DHCP request and make the necessary changes to the header, replacing the destination address with the address of the server, and the source with its own address, and send it to the server. When the response comes from the server, the DHCP/BOOTP relay function sends it to the host.

Purpose

To configure IP broadcast settings.

Commands

For information about...	Refer to page...
ip directed-broadcast	16-19
ip forward-protocol	16-20
ip helper-address	16-21

ip directed-broadcast

Use this command to enable or disable IP directed broadcasts on an interface.

Syntax

```
ip directed-broadcast
no ip directed-broadcast
```

Parameters

None.

Defaults

None.

Mode

Router command, Interface configuration: **Matrix>Router(config-if(Vlan 1))#**

Downloaded from www.Manualslib.com manuals search engine

Usage

The “no” form of this command disables IP directed broadcast globally.

Example

This example shows how to enable IP directed broadcasts on VLAN 1:

```
Matrix>Router(config)#interface vlan 1
Matrix>Router(config-if(Vlan 1))#ip directed-broadcast
```

ip forward-protocol

Use this command to enable UDP broadcast forwarding and specify which protocols will be forwarded.

Syntax

ip forward-protocol {**udp** [*port*]}

no ip forward-protocol {**udp** [*port*]}

Parameters

udp	Specifies UDP as the IP forwarding protocol.
port	(Optional) Specifies a destination port that controls which UDP services are forwarded. If not specified, the forwarding protocols are forwarded on the default ports listed: • Trivial File Transfer Protocol (TFTP) (port 69) • Bootstrap Protocol server (BootP) (port 67) • Domain Naming System (port 53) • Time service (port 37) • NetBIOS Name Server (port 137) • NetBIOS Datagram Server (port 138) • TACACS service (port 49) • EN-116 Name Service (port 42)

Defaults

If *port* is not specified, default forwarding services will be performed as listed above.

Mode

Router command, Global configuration: **Matrix>Router(config)#**

Usage

If a certain service exists inside the node, and there is no need to forward the request to remote networks, the “no” form of this command should be used to disable the forwarding for the specific port. Such requests will not be automatically blocked from being forwarded just because a service for them exists in the node.

The “no” form of this command removes a UDP port or protocol, disabling forwarding

Downloaded from www.Manualslib.com manuals search engine

Example

This example shows how to enable forwarding of Domain Naming System UDP datagrams (port 53):

```
Matrix>Router(config)#ip forward-protocol udp 53
```

ip helper-address

Use this command to enable DHCP/BOOTP relay and the forwarding of local UDP broadcasts specifying a new destination address.

Syntax

ip helper-address *address*

no ip helper-address *address*

Parameters

address	Specifies a destination broadcast of host address used when forwarding.

Defaults

None.

Mode

Router command, Interface configuration: **Matrix>Router(config-if(Vlan <vlan_id>))#**

Usage

This command works in conjunction with the **ip forward-protocol** command ("ip forward-protocol" on page 16-20), which defines the forward protocol and port number. You can use this command to add more than one helper address per interface.

The "no" form of this command disables the forwarding of UDP datagrams to the specified address

Example

This example shows how to permit UDP broadcasts from hosts on networks 191.168.1.255 and 192.24.1.255 to reach servers on those networks:

```
Matrix>Router(config)#ip forward-protocol udp
Matrix>Router(config)#interface vlan 1
Matrix>Router(config-if(Vlan 1))#ip helper-address 192.168.1.255
Matrix>Router(config)#interface vlan 2
Matrix>Router(config-if(Vlan 2))#ip helper-address 192.24.1.255
```


Downloaded from www.Manualslib.com manuals search engine

Reviewing IP Traffic and Configuring Routes

Purpose

To review IP protocol information about the device, to review IP traffic and configure routes, to enable and send router ICMP (ping) messages, and to execute traceroute.

Commands

For information about...	Refer to page...
show ip protocols	16-22
show ip traffic	16-23
clear ip stats	16-24
show ip route	16-25
ip route	16-26
ip icmp	16-27
ping	16-28
traceroute	16-28

show ip protocols

Use this command to display information about IP protocols running on the device.

Syntax

```
show ip protocols
```

Parameters

None.

Defaults

None.

Mode

Router command, Any router mode.

Usage

Enabling CIDR for RIP on the Enterasys Matrix Series device requires using the no auto-summary command (as described in “no auto-summary” on page 21-13) to disable automatic route summarization.

Downloaded from www.Manualslib.com manuals search engine

Example

This example shows how to display IP protocol information. In this case, the routing protocol is RIP (Routing Information Protocol). For more information on configuring RIP parameters, refer to "Configuring RIP" on page 21-1:

```
Matrix>Router#show ip protocols


Routing Protocol is "rip"
  Sending updates every 30 seconds
  Next due in 19 seconds
  Invalid after 180 seconds, hold down 120, flushed after 300
  Incoming update filter list for all interfaces is not set
  Outgoing update filter list for all interfaces is not set
  Default Version Control:
  Interface         Send        Recv        Key-chain
  Vlan    1         1           1
  Vlan    2         1           1
  Routing for Networks:
    182.127.0.0
  Routing Information Sources:
  Gateway         Distance        Last Update
  Distance: (default is 1)
```

show ip traffic

Use this command to display IP traffic statistics.

Syntax

show ip traffic [**softpath**]

Parameters

softpath	(Optional) Displays IP protocol softpath statistics. This option is used for debugging.

Defaults

If **softpath** is not specified, general IP traffic statistics will be displayed.

Mode

Router command, Any router mode.

Example

This example shows how to display IP traffic statistics

```
Matrix>Router#show ip traffic
IP Statistics:
  Rcvd:   10 total, 6 local destination 0 header errors
          0 unknown protocol, 0 security failures
```


Downloaded from www.Manualslib.com manuals search engine

```
          Frags:   0 reassembled, 0 timeouts 0 couldn't reassemble
                   0 fragmented, 0 couldn't fragment
  Bcast:  1 received, 8 sent
  Mcast:  0 received, 16 sent
  Sent:   24 generated, 0 forwarded
         0 no route
  ICMP Statistics:
    Rcvd:  4 total, 0 checksum errors, 0 redirects, 0 unreachable, 4 echo
              0 echo reply, 0 mask requests, 0 quench
              0 parameter, 0 timestamp, 0 time exceeded,
    Sent:  6 total, 0 redirects, 0 unreachable, 0 echo, 4 echo reply
              0 mask requests, 2 mask replies, 0 quench, 0 timestamp
0 info reply, 0 time exceeded, 0 parameter problem
  UDP Statistics:
    Rcvd:  1 total, 0 checksum errors, 1 no port
    Sent:  6 total, 0 forwarded broadcasts
  TCP Statistics:
    Rcvd:  0 total, 0 checksum errors, 0 no port
    Sent:  0 total
  IGMP Statistics:
    Rcvd:  Messages 1  Errors 0
        Reports 1   Queries 0
        Leaves 0    Unknowntype 0
   Sent: OutMessages 2
  ARP Statistics:
    Rcvd:  1 requests, 0 replies, 0 others
  Sent:  0 requests, 1 replies
```

clear ip stats

Use this command to clear all IP traffic counters (IP, ICMP, UDP, TCP, IGMP, and ARP).

Syntax

clear ip stats

Parameters

None.

Defaults

None.

Mode

Privileged EXEC: **Matrix>Router#**

Downloaded from www.Manualslib.com manuals search engine

Example

This example shows how to clear all IP traffic counters:

```
Matrix>Router#clear ip stats
```

show ip route

Use this command to display information about IP routes.

Syntax

show ip route [*destination prefix destination prefix mask* **longer-prefixes** | **connected** | **ospf** | **rip** | **static** | **summary**]

Parameters

destination prefix destination prefix mask **longer-prefixes**	(Optional) Converts the specified address and mask into a prefix and displays any routes that match the prefix.
connected	(Optional) Displays connected routes.
ospf	(Optional) Displays routes configured for the OSPF routing protocol. For details on configuring OSPF, refer to "Configuring OSPF" on page 21-19.
rip	(Optional) Displays routes configured for the RIP routing protocol. For details on configuring RIP, refer to "Configuring RIP" on page 21-1.
static	(Optional) Displays static routes.
summary	(Optional) Displays a summary of the IP routing table.

Defaults

If no parameters are specified, all IP route information will be displayed.

Mode

Router command, Any router mode.

Usage

When there is more than one routing module configured in an Enterasys Matrix chassis, each module will create and maintain its own route tables.

Routes are managed by the RTM (Route Table Manager), and are contained in the RIB (Route Information Base). This database contains all the active static routes, all the RIP routes, and up to three best routes to each network as determined by OSPF.

The RTM selects up to three of the best routes to each network and installs these routes in the FIB (Forwarding Information Base). The routes in the FIB are distributed to every module for use by the router's distributed forwarding engine on the ingress module as frames are received.

Downloaded from www.Manualslib.com manuals search engine

Example

This example shows how to display all IP route information. In this case, there are routes directly connected to VLANs 1 and 2, two static routes connected to VLAN 1 (one indirectly, and one via another network IP), and one RIP route. Distance/cost is displayed as [x/y]:

```
Matrix>Router#show ip route
Codes: C -  connected, S -  static,  R - RIP, O - OSPF, IA - OSPF inter area, N1
- OSPF NSSA external type 1, N2 - OSPF NSSA external type 2, E1 - OSPF external
type 1, E2 - OSPF external type 2, * - candidate default, U - per user static route

C         192.168.27.0/24           [    0/0001] directly connected, vlan 1
C         192.168.32.0/24           [    0/0001] directly connected, vlan 2
S          2.0.0.0/8                [   65/0001] via 192.168.72.1, vlan 1
S          3.0.0.0/8                [    0/0001] directly connected vlan 1
R          1.0.0.0/8                [   70/0002] via 192.168.72.22 vlan 1
```

ip route

Use this command to add or remove a static IP route.

Syntax

ip route *prefix mask* {*forward-addr* | **vlan** *vlan-id*} [*distance*] [**permanent**] [**tag** *value*]

no ip route *prefix mask* {*forward-addr* | **vlan** *vlan-id*}

Parameters

prefix	Specifies a destination IP address prefix.
mask	Specifies a destination prefix mask.
forward-addr | **vlan** *vlan-id*	Specifies a forwarding (gateway) IP address or routing (VLAN) interface ID.
distance	(Optional) Specifies an administrative distance metric for this route. Valid values are **1** (default) to **255**. Routes with lower values receive higher preference in route selection.
permanent	(Optional) Specifies a permanent route.
tag *value*	(Optional) Specifies a tag for this route. Valid values are **1** to **4294967295**.

Defaults

- If *distance* is not specified, the default value of 1 will be applied.
- If **permanent** and **tag** are not specified, the route will be set as non-permanent with no tag assigned.

Mode

Router command, Global configuration: **Matrix>Router(config)#**

Usage

The “no” form of this command removes the static IP route.

Downloaded from www.Manualslib.com manuals search engine

Examples

This example shows how to set IP address 10.1.2.3 as the next hop gateway to destination address 10.0.0.0. The route is assigned a tag of 1:

```
Matrix>Router(config)#ip route 10.0.0.0 255.0.0.0 10.1.2.3 1
```

This example shows how to set IP address 10.1.2.3 as the next hop gateway to destination address 10.0.0.0. The route is set as permanent and assigned a tag of 20:

```
Matrix>Router(config)#ip route 10.0.0.0 255.0.0.0 10.1.2.3 permanent tag 20
```

This example shows how to set VLAN 100 as the next hop interface to destination address 10.0.0.0:

```
Matrix>Router(config)#ip route 10.0.0.0 255.0.0.0 vlan 100
```

ip icmp

Use this command to re-enable the Internet Control Message Protocol (ICMP), allowing a router to reply to IP ping requests.

Syntax

ip icmp {**echo-reply** | **mask-reply**}

no ip icmp {**echo-reply** | **mask-reply**}

Parameters

echo-reply	Enables ICMP in echo-reply mode.
mask-reply	Enables ICMP in mask-reply mode.

Defaults

None.

Mode

Router command, Interface configuration: **Matrix>Router(config-if(Vlan 1))#**

Usage

By default, ICMP messaging is enabled on a routing interface for both echo-reply and mask-reply modes. If, for security reasons, ICMP has been disabled using **no ip icmp**, this command will re-enable it on the routing interface.

The “no” form of this command disables ICMP.

Example

This example shows how to enable ICMP in echo-reply mode on VLAN 1:

```
Matrix>Router(config)#interface vlan 1
Matrix>Router(config-if(Vlan 1))#ip icmp echo-reply
```


Downloaded from www.Manualslib.com manuals search engine

ping

Use this command to test routing network connectivity by sending IP ping requests.

Syntax

ping *ip-address*

Parameters

ip-address	Specifies the IP address of the system to ping.

Defaults

None.

Mode

Router command, Privileged EXEC: **Matrix>Router#**

Usage

The ping utility (IP ping only) transmits a maximum of five echo requests, with a packet size of 100. The application stops when the response has been received, or after the maximum number of requests has been sent

Examples

This example shows output from a successful ping to IP address 182.127.63.23:

```
Matrix>Router#ping 182.127.63.23
Reply from 182.127.63.23
Reply from 182.127.63.23
Reply from 182.127.63.23

------ PING 182.127.63.23 : Statistics ------
 3 packets transmitted, 3 packets received, 0% packet loss
```

This example shows output from an unsuccessful ping to IP address 182.127.63.24:

```
Matrix>Router#ping 182.127.63.24
Timed Out
Timed Out
Timed Out

 ------ PING 182.127.63.24 : Statistics ------
 3 packets transmitted, 0 packets received, 100% packet loss
```

traceroute

Use this command to display a hop-by-hop path through an IP network from the device to a specific destination host.

Syntax

traceroute *host*

Downloaded from www.Manualslib.com manuals search engine

Parameters

host	Specifies a host to which the route of an IP packet will be traced.

Defaults

None.

Mode

Router command, Privileged EXEC: **Matrix>Router#**

Usage

Three ICMP probes will be transmitted for each hop between the source and the traceroute destination.

Examples

This example shows how to use traceroute to display a round trip path to host 192.167.252.46. In this case, hop 1 is an unnamed router at 192.167.201.2, hop 2 is "rtr10" at 192.4.9.10, hop 3 is "rtr43" at 192.167.208.43, and hop 4 is back to the host IP address. Round trip times for each of the three ICMP probes are displayed before each hop. Probe time outs are indicated by an asterisk (*):

```
Matrix>Router#traceroute 192.167.225.46

Traceroute to 192.167.225.46, 30 hops max, 40 byte packets
1  10.00 ms  20.00 ms  20.00 ms  192.167.201.2 []
2  20.00 ms  20.00 ms  20.00 ms  192.4.9.10 [enatel-rtr10.enatel.com]
3  240.00 ms  *         480.00 ms  192.167.208.43 [enatel-rtr43.enatel.com]
4  <1 ms     *         20.00 ms  192.167.225.46 [enatel-rtr46.enatel.com]

TraceRoute Complete
```


Downloaded from www.Manualslib.com manuals search engine

Configuring Debug IP Packet

Purpose

Debug IP packet is an IP based packet monitor that allows for the monitoring of all IP traffic received and transmitted from an N-Series router forwarding engine. Debug IP Packet uses SYSLOG messages to display packet information. Packet filtering takes place by assigning a router access group to the **debug ip packet** command and is based on the groups ACL entries. This utility displays matching frames for the defined signature being processed in the soft path of the router. It is desirable that the number of rules assigned to the access group be limited so as to minimize the impact on the forwarding system performance. By default the utility displays a subset of available information. A verbose option provides detailed packet information. Options are available to both throttle the number of packets per second and limit the number of packets per board.

Commands

For information about...	Refer to page...
debug ip packet access-group	16-30
debug ip packet restart	16-31
show debugging	16-32
no debug ip packet	16-32

debug ip packet access-group

Use this command to enable the debug IP packet utility for monitoring of IP packets based upon the associated access-group.

Syntax

debug ip packet access-group *access-group* [**throttle** *throttle*] [**limit** *limit*] [**verbose**]

Parameters

access-group	Specifies the name of the access group used to filter packets for this command.
throttle *throttle*	(Optional) Specifies the number of filtered packets per second to be displayed. Valid Values: **2** - **100**
limit *limit*	(Optional) Specifies the number of packets per board to be displayed. Valid Values: **0** - **1000** (**0** = no limit applied)
verbose	(Optional) Specifies detailed packet information level.

Defaults

throttle = **10,** limit = **30**.

Downloaded from www.Manualslib.com manuals search engine

Mode

Router command, Router configuration: **Matrix>Router(config)#**
Router Exec: **Matrix>Router#**

Usage

- Too high a throttle or limit value may require a second CLI session for CLI access due to the volume of potential data.
- Use the **debug ip packet restart** command to restart the utility when the display limit has been reached.
- Before entering this command, enter a **set logging here enable** command at the Read-Write command prompt to direct SYSLOG messages to this session.
- The current state of IP debugging is not displayed by the **show running-config** command. It is not a persistently saved configuration. To see the state of this command use the **show debugging** command.

Example

This example shows how to set debug IP packet for throttle 5 and limit 20 with a detail value of verbose:

```
Matrix(rw)->set logging here enable
Opened (71) at index 5
Matrix(rw)->router
Matrix(rw)->Router>enable
Matrix(rw)->Router#configure
Matrix(rw)->Router(config)#access-list 1 permit any
Matrix(rw)->Router(config)#debug ip packet access-group 1 throttle 5 limit 20
verbose
<165>Jun 26 13:53:03 65.41.41.41 DbgIpPkt[1.tDispEvent][2][Snd]Rule hit[1: permit
any] out vlan 2730
<165>Jun 26 13:53:04 65.41.41.41 DbgIpPkt[2.tDispEvent][1][Rcv]Rule hit[1: permit
any] PortSting empty for port-21 vlan 2730
<165>Jun 26 13:53:04 65.41.41.41 DbgIpPkt[2.tDispEvent][2][Rcv]Rule hit[1: permit
any] PortSting empty for port-21 vlan 2730
<165>Jun 26 13:53:05 65.41.41.41 DbgIpPkt[3.tDispEvent][1][Rcv]Rule hit[1: permit
any] PortSting empty for port-69 vlan 2730
.
.
.
Matrix(rw)->Router(config)#show debug
IP Packet debugging is on, with access-group 1 throttle 5 limit 20 verbose
Matrix(rw)->Router(config)#
```

debug ip packet restart

Use this command to restart the debug IP packet utility.

Syntax

debug ip packet restart

Downloaded from www.Manualslib.com manuals search engine

Parameters

None.

Defaults

None.

Mode

Router command, Router configuration: **Matrix>Router(config)#**
Router Exec: **Matrix>Router#**

Usage

By default, 30 packet will be display and then the packet monitor will stop. To collect another 30 packets, use this command. The default of 30 can be modified with the **debug ip packet access-group limit** parameter.

Example

This example shows how to restart the debug IP packet utility:

```
Matrix(rw)->Router(config)#debug ip packet restart
```

show debugging

Use this command to display the debug IP Packet utility settings.

Syntax

show debugging

Parameters

None.

Defaults

None.

Mode

Router command, Router configuration: **Matrix>Router(config)#**

Example

This example shows how to display the debug IP packet utility settings:

```
Matrix(rw)->Router(config)#show debug
IP Packet debugging is on, with access-group 1 throttle 5 limit 20 verbose
```

no debug ip packet

Use this command to disable the debug IP packet utility.

Syntax

no debug ip packet

Downloaded from www.Manualslib.com manuals search engine

Parameters

None.

Defaults

None.

Mode

Router command, Router configuration: **Matrix>Router(config)#**

Example

This example shows how to disable the debug IP packet utility:

```
Matrix(rw)->Router(config)#no debug ip packet
```


Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

17

PIM Configuration

This chapter describes the Protocol Independent Multicast (PIM) configuration set of commands and how to use them.



Router: Unless otherwise noted, the commands covered in this chapter can be executed only when the device is in router mode. For details on how to enable router configuration modes, refer to "Enabling Router Configuration Modes" on page 2-103.

Configuring PIM

Important Notice

PIM is an advanced routing feature that must be enabled with a license key. If you have purchased an advanced license key, and have enabled routing on the device, you must activate your license as described back in "Activating Licensed Features" on page 2-58 in order to enable the PIM command set. If you wish to purchase an advanced routing license, contact Enterasys Networks Sales.

Purpose

To review and configure Protocol Independent Multicast (PIM).

Commands

For information about...	Refer to page...
ip pim sparse mode	17-2
ip pim bsr-candidate	17-2
ip pim dr-priority	17-3
ip pim rp-address	17-4
ip pim rp-candidate	17-5
show ip pim bsr	17-5
show ip pim interface	17-6
show ip pim neighbor	17-7
show ip pim rp	17-8
show ip pim rp-hash	17-10
show ip mroute	17-10

Downloaded from www.Manualslib.com manuals search engine

For information about...	Refer to page...
show ip mforward	17-11
show ip rpf	17-12

ip pim sparse mode

Use this command to enable Protocol Independent Multicast (PIM) Sparse Mode (SM) on a routing interface.

Syntax

ip pim sparse-mode

no ip pim sparse-mode

Parameters

None.

Defaults

None.

Mode

Router command, Interface configuration: **Matrix>Router(config-if(Vlan 1))#**

Usage

The “no” form of this command disables PIM on an interface.

Example

This example enables PIM sparse mode on VLAN 1:

```
Matrix>Router(config)#interface vlan 1
Matrix>Router(config-if(Vlan 1))#ip pim sparse-mode
```

ip pim bsr-candidate

Use this command to enable the router to announce its candidacy as a BootStrap Router (BSR).

Syntax

ip pim bsr-candidate *pim-interface* [*hash-mask-length*] [*priority*]]

no ip bsr-candidate

Downloaded from www.Manualslib.com manuals search engine

Parameters

pim-interface	Interface of the BSR candidate. This interface must be enabled with PIM as described in "ip pim sparse mode" on page 17-2.
hash-mask-length	(Optional) Length of a mask to be added with the group address before the hash function is called. All groups with the same seed hash correspond to the same Rendezvous Point (RP). This option provides one RP for multiple groups. A *hash-mask-length* value of **30** will be automatically applied.
priority	(Optional) Specifies a BSR priority value ranging from **0** - **255**. Higher values assign higher priority. The BSR with the larger priority is preferred. If priority values are the same, the IP address breaks the tie. The BSR candidate with the higher IP address is preferred.

Defaults

- A *hash-mask-length* value of 30 will be automatically applied.
- If *priority* is not specified, **1** will be applied.

Mode

Router command, Interface configuration: **Matrix>Router(config-if(Vlan 1))#**

Usage

The "no" form of this command removes the router as a BSR candidate.

Example

This example sets the hash mask length to 30 and DR priority to 77 on VLAN 1:

```
Matrix>Router(config)#interface vlan 1
Matrix>Router(config-if(Vlan 1))#ip pim bsr-candidate vlan 1 priority 77
```

ip pim dr-priority

Use this command to set the priority for which a router will be elected as the designated router (DR).

Syntax

ip pim dr-priority *priority*

no ip dr-priority

Parameters

priority	Specifies a priority value for designated router selection. Valid values are **0** - **4294967294**. Default is **1**.

Defaults

None.

Downloaded from www.Manualslib.com manuals search engine

Mode

Router command, Interface configuration: **Matrix>Router(config-if(Vlan 1))#**

Usage

The "no" form of this command disables the DR functionality.

Example

This example sets the DR priority to 20 on VLAN 1:

```
Matrix>Router(config)#interface vlan 1
Matrix>Router(config-if(Vlan 1))#ip pim dr-priority 20
```

ip pim rp-address

Use this command to set a static rendezvous point (RP) for a multicast group.

Syntax

ip pim rp-address *rp-address group-address group-mask* [**priority** *priority*]

no ip rp-address *rp-address group-address group-mask*

Parameters

rp-address	Specifies the IP address of the PIM RP router.
group-address	Specifies the multicast group address.
group-mask	Specifies the multicast group mask.
priority *priority*	(Optional) Specifies an RP priority value, ranging from **0** - **255**. Lower values assign higher priority.

Defaults

If not specified, a *priority* value of 192 will be assigned.

Mode

Router command, Global configuration: **Matrix>Router(config)#**

Usage

The "no" form of this command removes the static RP configuration.

Example

This example sets a static RP address at 10.0.0.1 for the multicast group at 235.0.0 255.0.0:

```
Matrix>Router(config)#ip pim rp-address 10.0.0.1 235.0.0.0. 255.0.0.0
```


Downloaded from www.Manualslib.com manuals search engine

ip pim rp-candidate

Use this command to enable the router to advertise itself as a PIM candidate rendezvous point (RP) to the BSR.

Syntax

ip pim rp-candidate *pim-interface group-address group-mask* [**priority** *priority*]

no ip pim rp-candidate *pim-interface group-address group-mask*

Parameters

pim-interface	Interface to advertise as an RP candidate. This interface must be enabled with PIM as described in "ip pim sparse mode" on page 17-2.
group-address	Specifies the multicast group address.
group-mask	Specifies the multicast group mask.
priority *priority*	(Optional) Specifies an RP priority value, ranging from **0** - **255**. Lower values assign higher priority.

Defaults

If not specified, a DR *priority* value of 192 will be assigned.

Mode

Router command, Global configuration: **Matrix>Router(config)#**

Usage

Only one RP candidate can be configured per routing module or standalone device.

The "no" form of this command removes the router as an RP candidate.

Example

This example enables the PIM interface at 35.0.0 224.0.0 240.0.0 to advertise itself as an RP candidate with a priority of 124:

```
Matrix>Router(config)#ip pim rp-candidate 35.0.0.1 224.0.0.0 240.0.0.0 priority
124
```

show ip pim bsr

Use this command to display BootStrap Router (BSR) information.

Syntax

show ip pim bsr

Parameters

None.

Defaults

None.

Downloaded from www.Manualslib.com manuals search engine

Mode

Router command, Privileged EXEC: **Matrix>Router#**

Example

This example shows how to display BootStrap Router (BSR) information:

```
Matrix>Router#show ip pim bsr

PIMv2 Elected Bootstrap Router Information:
BSR Address: 10.0.0.1
Bsr Priority: 77
Bsr Hash Mask Length: 30
Bsr Uptime: 00:01:10
Bsr Expiry: 00:00:49

This Router is a Candidate Bootstrap Router (CBSR)
Candidate BSR Address: 10.0.0.1
Hash Mask Length: 30
Priority: 77
```

Table 17-1 provides an explanation of the command output.

Table 17-1 show ip pim bsr Output Details

Output...	What it displays...
BSR Address	IP address of the bootstrap router.
BSR Priority	Priority as set by the **ip pim bsr-candidate** command.
BSR Hash Mask Length	Length of a mask (32 bits maximum) that is to be added with the group address before the hash function is called. This value is configured by the **ip pim bsr-candidate** command.
BSR Uptime	Interval that this router has been up (in hours:minutes:seconds). After 24 hours, format will change into days:hours and, after a week, will change into weeks:days.
BSR Expiry	Period in which the next bootstrap message is due from this BSR (in hours:minutes:seconds). After 24 hours, format will change into days:hours and, after a week, will change into weeks:days. Assigning a time value of 00:00:00 means this BSR will not expire.

show ip pim interface

Use this command to display information about PIM interfaces that are currently up (not shutdown).

Syntax

show ip pim interface [*interface*]

Downloaded from www.Manualslib.com manuals search engine

Parameters

interface	(Optional) Displays information about a specific PIM interface. This interface must be enabled with PIM as described in "ip pim sparse mode" on page 17-2.

Defaults

If not specified, information about all PIM interfaces will be displayed.

Mode

Router command, Privileged EXEC: **Matrix>Router#**

Example

This example shows how to display PIM interface information

```
Matrix>Router#show ip pim interface

Address         Vlan    Ver/Mode Nbr-Count Query-Intvl DR-Prior    DR
------------------------------------------------------------------------------
 35.0.0.1        35       v2/S     1         30          1        35.0.0.2
 23.0.0.1        23       v2/S     0         30          1        23.0.0.1
 20.0.0.2        20       v2/S     0         30          1        20.0.0.2
 10.0.0.1        10       v2/S     2         30          87       10.0.0.1
```

Table 17-2 provides an explanation of the command output.

Table 17-2 show ip pim interface Output Details

Output...	What it displays...
Address	IP address of the PIM interface.
Vlan	VLAN ID of the PIM interface.
Ver/Mode	Version and mode (sparse or dense) of PIM running on the interface.
Nbr-Count	Total number of PIM neighbors on the interface, discovered by receiving PIM hello messages from other PIM routers on the interface.
Query-Intvl	Interval between Hello messages. Default is 30 seconds.
DR-Prior	Designated router priority value on the interface. Set with the **ip pim dr-priority** command ("ip pim dr-priority" on page 17-3).
DR	IP address of the designated router on the LAN.

show ip pim neighbor

Use this command to display information about discovered PIM neighbors.

Syntax

show ip pim neighbor [*interface*]

Downloaded from www.Manualslib.com manuals search engine

Parameters

interface	(Optional) Displays information about a specific PIM interface. This interface must be enabled with PIM as described in "ip pim sparse mode" on page 17-2.

Defaults

If not specified, information about all PIM interfaces will be displayed.

Mode

Router command, Privileged EXEC: **Matrix>Router#**

Example

This example shows how to display PIM neighbor information:

```
Matrix>Router#show ip pim neighbor

Neighbor Address    Vlan    DR Priority    Uptime      Expires       Mode ------
--------------------------------------------------------------------------
10.0.0.2            10      1              00:03:34    00:01:40    PIMSM_MODE (DR)
```

Table 17-3 provides an explanation of the command output.

Table 17-3 show ip pim neighbor Output Details

Output...	What it displays...
Neighbor Address	IP address of the PIM neighbor.
Vlan	VLAN ID of the PIM interface.
DR Priority	DR priority of the neighbor.
Uptime	Interval in hours, minutes, and seconds the entry has been in the PIM neighbor table.
Expires	Interval in hours, minutes, and seconds until the entry will be removed from the IP multicast routing table.
Mode	Mode in which the interface is operating.
(DR)	Indicates that this neighbor is a designated router on the LAN.

show ip pim rp

Use this command to display the active rendezvous points (RPs) that are cached with associated multicast routing entries.

Syntax

show ip pim rp [**group** | **mapping** | *multicast-group-address*]

Downloaded from www.Manualslib.com manuals search engine

Parameters

group	(Optional) Displays active RPs for any existing multicast group(s).
mapping	(Optional) Displays all RP mappings.
multicast-group-address	(Optional) Displays RP information for a specific multicast group IP address.

Defaults

If no optional parameters are specified, all active RPs will be displayed.

Mode

Router command, Privileged EXEC: **Matrix>Router#**

Examples

This example shows how to display information about active RPs:

```
Matrix>Router#show ip pim rp
Group: 225.1.2.3, RP: 192.168.41.1, uptime 07:49:53, expires 00:02:09
```

This example shows how to display RP mapping information:

```
Matrix>Router#show ip pim rp mapping
PIM Group to RP Mapping:

    Group(s): 228.3.3.3/32
        RP: 41.41.1.1, via Static Configuration

    Group(s): 224.0.0.0/4
        RP: 192.168.41.1, Priority:   2, Expiry: 00:01:30, Uptime: 07:49:31
        RP: 192.168.91.1, Priority:   5, Expiry: 00:01:30, Uptime: 07:49:31
```

Table 17-4 provides an explanation of the command output.

Table 17-4 show ip pim rp Output Details

Output...	What it displays...
Group(s)	Address of the multicast group(s) about which to display RP data.
RP	Address of the RP for that group.
Priority	RP priority value.
Expiry	Period (in hours:minutes:seconds) in which the next bootstrap message is due from this BSR.
Uptime	Interval that this router has been up in hours:minutes:seconds.

Downloaded from www.Manualslib.com manuals search engine

show ip pim rp-hash

Use this command to display the rendezvous point (RP) that is being selected for a specified group.

Syntax

show ip pim rp-hash *group-address*

Parameters

group-address	Displays information about a specific group address.

Defaults

None.

Mode

Router command, Privileged EXEC: **Matrix>Router#**

Example

This example shows how to display RP hash information:

```
Matrix>Router#show ip pim rp-hash
RP  192.168.41.1, via  Bootstrap Router, uptime 07:50:10, expires 00:01:52
```

show ip mroute

Use this command to display the IP multicast routing table.

Syntax

show ip mroute [*unicast-source-address* | *multicast-group-address*] [**summary**]

Parameters

unicast-source-address | *multicast-group-address*	(Optional) Displays information about a specific unicast source address or multicast destination address.
summary	(Optional) Displays a summary of information.

Defaults

If no optional parameters are specified, detailed information about all source and destination addresses will be displayed.

Mode

Router command, Any router mode.

Usage

This table shows how a multicast routing protocol, such as PIM and DVMRP, will forward a multicast packet. Information in the table includes source network/mask and upstream neighbors. For more information on configuring DVMRP, refer to "Configuring DVMRP" on page 21-52.

Downloaded from www.Manualslib.com manuals search engine

Example

This example shows a portion of the IP multicast routing table display. In this case, it shows there are nine source PIM sparse mode (PIMSM) multicast networks. PIMSM network 1 shows an incoming route at VLAN-999 and outgoing routes at VLANs 410, 555, 910 and 920:

```
Matrix>Router#show ip mroute
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, C - Connected, L - Local, P - Pruned
       R - RP-bit set, F - Register flag, T - SPT-bit set, J - Join SPT
Timers: Uptime/Expires
Interface state: Interface, Next-Hop or VCD, State/Mode

1 of 9: PIMSM (*, 225.1.2.3), 01:52:43/00:02:33, RP 192.168.41.1, flags: SC
       Incoming interface: Vlan-999, RPF nbr 99.99.1.1
       Outgoing interface list:
         Vlan-410, Forward/Sparse, 01:52:43/00:00:00
         Vlan-555, Forward/Sparse, 01:48:54/00:02:33
         Vlan-910, Forward/Sparse, 01:52:43/00:00:00
         Vlan-920, Forward/Sparse, 01:52:43/00:00:00
```

show ip mforward

Use this command to display the IP multicast forwarding table.

Syntax

show ip mforward [*unicast-source-address* | *multicast-group-address*] [**summary**]

Parameters

unicast-source-address | *multicast-group-address*	(Optional) Displays information about a specific unicast source address or multicast destination address.
summary	(Optional) Displays a summary of information.

Defaults

If no optional parameters are specified, detailed information about all source and destination addresses will be displayed.

Mode

Router command, Any router mode.

Usage

This table shows what multicast routes have actually been programmed into the Enterasys Matrix hardware. Although redundant to the **show ip mroute** display ("show ip mroute" on page 17-10), it is a useful debugging tool if there are discrepancies between the multicast routing table and the multicast forwarding table.

Downloaded from www.Manualslib.com manuals search engine

Example

This example shows a portion of the IP multicast forwarding table display:

```
Matrix>Router#show ip mforward
IP Multicast Forwarding Table

1 of 8: (63.63.100.1/32, 225.1.2.3)
Sources: 63.63.100.1
Incoming interface: Vlan-999
Outgoing interface list:
Vlan-410, Forward/Sparse
Vlan-555, Forward/Sparse
Vlan-910, Forward/Sparse
Vlan-920, Forward/Sparse
```

show ip rpf

Use this command to display the reverse path of an address in the unicast table.

Syntax

show ip rfp

Parameters

None.

Defaults

None.

Mode

Router command, Any router mode.

Example

This example shows the reverse path information for IP address 80.80.80.252.

```
Matrix(rw)->Router2>show ip rpf 80.80.80.252

RPF information for: 80.80.80.252
    RPF vlan interface: 10
    RPF route/mask:192.168.1.0/255.255.255.0
    RPF neighbor:192.168.1.25
    Metric preference:110
    Metric:10
```


Downloaded from www.Manualslib.com manuals search engine

18

Network Address Translation (NAT) Configuration

This chapter describes the Network Address Translation (NAT) configuration set of commands and how to use them.



Router: Unless otherwise noted, the commands covered in this chapter can be executed only when the device is in router mode. For details on how to enable router configuration modes, refer to "Enabling Router Configuration Modes" on page 2-103.



Note: An Enterasys Feature Guide document that contains a complete discussion on NAT configuration exists at the following Enterasys web site: http://www.enterasys.com/support/manuals/

Configuring Network Address Translation (NAT)

The Enterasys Network Address Translation (NAT) implementation supports Basic NAT and Network Address Port Translation (NAPT). In addition, the following features are also supported:

- Static and Dynamic NAT Pool Binding
- FTP, DNS, TELNET, SSH, TFTP, HTTP, NTP (Network Time Protocol), and ICMP (with five different error messages) software path NAT translation
- Force Flows (Secure Plus)

Both basic NAT and NAPT are referred to as traditional NAT and provide a mechanism to connect a realm with private addresses to an external realm with globally unique registered addresses. Basic NAT is a method by which IP addresses are mapped from one group to another, transparent to the end user. NAPT is a method by which many network addresses, along with their associated TCP/UDP ports, are translated into a single network address and its associated TCP/UDP ports.

The static address binding feature is designed for both the basic NAT and NAPT implementations to support static and no expire binding, between inside and outside NAT address translation. It supports one-to-one binding, local addresses to global addresses, and TCP/UDP port number translations.

The dynamic address binding feature is designed for both the basic NAT and NAPT implementations to support dynamic binding between an address from an access-list of local addresses to an address from a pool of global addresses. IP addresses defined for dynamic binding are reassigned whenever they become available from the global address pool. NAPT allows port address translation for each IP address in the global pool. The ports are dynamically assigned between a range of 1024 to 4999.

It is sometimes possible for a host on the outside global network that knows an inside local address, to be able to send a message directly to the inside local address without NAT translation. The force flows feature, set using the command *ip nat secure-plus* on page 18-7, is designed to force all flows between the inside local pool and the outside global network to be translated.

Downloaded from www.Manualslib.com manuals search engine

NAT works with DNS by having the DNS Application Specific Gateway (ALG) translate an address that appears in a Domain Name System response to a name or inverse lookup.

NAT works with FTP by having the FTP ALG translate the FTP control payload. Both FTP PORT CMD packets and PASV packets, containing IP address information within the data portion, are supported.

The NAT implementation also supports the translation of the IP address embedded in the data portion of following types of ICMP error message: destination unreachable (type3), source quench (type4), redirect (type5), time exceeded (type 11) and parameter problem (type 12).

Purpose

To display and set NAT and NAPT configuration including dynamic pools, static and dynamic NAT configurations, FTP control port, Force Flows, maximum entries and timeout values, and clear active translations.

NAT Configuration Task List and Commands

Table 18-1 lists the mandatory and optional tasks and commands for configuring NAT on the Enterasys Matrix Series device. Commands are described in the associated sections as shown.

Table 18-1 NAT Configuration Task List and Commands

Task	Use these commands...
Enable NAT on an inside or outside interface.	**ip nat** {**inside** | **outside**}
Define a NAT address pool.	**ip nat pool** *name start-ip-address end-ip-address* {**netmask** *netmask* | **prefix-length** *prefix-length*}
Enable dynamic translation of inside source addresses.	**ip nat inside source** [**list** *access-list*] **pool** *pool-name* [**overload** | **interface vlan** *vlan-id* [**overload**]]
Enable static NAT translation of inside source addresses.	**ip nat inside source static** *local-ip global-ip*
Enable static NAPT translation of inside source addresses.	**ip nat inside source static** {**tcp** | **udp**} *local-ip local-port global-ip global-port*
Specify the NAT FTP control port.	**ip nat ftp-control-port** *port-number*
Block the defined inside IP addresses from ever appearing on an outside interface.	**ip nat secure-plus**
Configure the maximum number of translation entries.	**ip nat translation max-entries** *number*
Configure NAT translation timeout values.	**ip nat translation** {**timeout | udp-timeout | tcp-timeout | icmp-timeout | dns-timeout | ftp-timeout**} *seconds*
Display active NAT translations.	**show ip nat translations** [**verbose**]
Display NAT translation statistics.	**show ip nat statistics** [**verbose**]
Clear dynamic NAT translations.	**clear ip nat translation**
Clear a specific active simple NAT translation.	**clear ip nat translation inside** *global-ip local-ip*
Clear a specific dynamic NAT translation.	**clear ip nat translation** {**tcp** | **upd**} **inside** *global-ip global-port local-ip local-port*

Downloaded from www.Manualslib.com manuals search engine

ip nat

Use this command to enable NAT on this interface.

Syntax

ip nat {**inside** | **outside**}

no ip nat {**inside** | **outside**}

Parameters

inside	Specifies that this internal network interface should be enabled for NAT as a private interface.
outside	Specifies that this external network interface should be enabled for NAT as a public interface.

Defaults

None.

Mode

Router command, Interface configuration: **Matrix->Router(config-if)#**.

Usage

This command designates that traffic originating from or destined for the interface is subject to NAT.

The no version of the command disables NAT for the specified interface type.

Example

This example enables interface **VLAN 1** as an inside NAT interface:

```
Matrix(rw)->router
Matrix->router>enable
Matrix->router#configure terminal
Enter configuration commands:
Matrix->Router(config)#interface vlan 1
Matrix->Router(config-if(Vlan 1))#ip nat inside
Matrix->Router(config-if(Vlan 1))#
```

ip nat pool

Use this command to define a NAT address pool used by the dynamic address binding feature for NAT translation.

Syntax

ip nat pool *name start-ip-address end-ip-address* [**netmask** *netmask* | **prefix-length** *prefix-length*]

no ip nat pool *name* [*start-ip-address end-ip-address*] [**netmask** *netmask* | **prefix-length** *prefix-length*]

Downloaded from www.Manualslib.com manuals search engine

Parameters

name	Specifies the name of this NAT pool.
start-ip-address	Specifies the start of the IP address range for members of this NAT pool.
end-ip-address	Specifies the end of the IP address range for members of this NAT pool.
netmask	(Optional) Specifies the netmask for this NAT pool range.
prefix-length	(Optional) Specifies the prefix length for this NAT pool range.

Defaults

If no netmask or prefix-length is specified, all addresses in the range are used.

Mode

Router command, Global configuration: **Matrix->Router(config)#**

Usage

The dynamic address binding feature draws interfaces from a specified NAT pool. The netmask and prefix-length parameters are optional. If no values are given, a host route will be added for each IP address in the pool. If either parameter is given, the IP address range will be checked against the netmask and a network route will be added for this pool.

The no version of the command deletes the specified NAT pool.

Example

This example defines the **doc1** NAT address pool with a start address of **10.10.10.25** and end address of **10.10.10.45** and a netmask of **255.255.255.0**:

```
Matrix->Router(config)#ip nat pool doc1 10.10.10.25 10.10.10.45 netmask
255.255.255.0
```

ip nat inside source list

Use this command to enable dynamic translation of inside source addresses.

Syntax

ip nat inside source list *access-list* **pool** *pool-name* [**overload** | **interface vlan** *vlan-id* [**overload**]]

no ip nat inside source list *access-list* **pool** *pool-name* [**overload** | **interface vlan** *vlan-id* [**overload**]]

Parameters

access-list	Specifies an access-list of IP addresses to translate for this inside source address.
pool-name	Specifies a pool of IP addresses to translate for this outside address
vlan-id	(Optional) Specifies the VLAN to which a translation is applied.

Defaults

If **overload** is not specified, NAT translation occurs. If **interface vlan** is not specified, translation is enabled on all VLANs.

Downloaded from www.Manualslib.com manuals search engine

Mode

Router command, Global configuration: **Matrix->Router(config)#**

Usage

Packets from addresses that match those on the specified access list are translated using global addresses allocated from the named pool. The optional **overload** key enables NAPT translation. The optional interface VLAN parameter ensures that the translation only applies to packets being transmitted out the specified VLAN.

The no version of the command disables dynamic translation of inside source addresses for the specified NAT pool.

Example

This example enables dynamic translation of inside interfaces for packets matching access list **1** criteria with IP addresses matching pool **doc1** on interface **vlan 1**:

```
Matrix->Router(config)#ip nat inside source list 1 pool doc1 interface vlan 1
```

ip nat inside source static (NAT)

Use this command to enable static NAT translation of inside source addresses.

Syntax

ip nat inside source static *local-ip global-ip*

no ip nat inside source static *local-ip global-ip*

Parameters

local-ip	Specifies the private (local) address to be associated with a public (global) address for this translation.
global-ip	Specifies the public (global) address to be associated with a private (local) address for this translation.

Defaults

None.

Mode

Router command, Global configuration: **Matrix->Router(config)#**

Usage

The no version of the command deletes the specified static NAT translation.

Example

This example enables a static NAT translation of inside source addresses for private local address **10.10.10.50** destined for and transmitting from unique public address **45.20.10.5**:

```
Matrix->Router(config)#ip nat inside source static 10.10.10.50 45.20.10.5
```


Downloaded from www.Manualslib.com manuals search engine

ip nat inside source static (NAPT)

Use this command to enable static NAPT translation of inside source addresses.

Syntax

ip nat inside source static {**tcp** | **udp**} *local-ip local-port global-ip global-port*

no ip nat inside source static {**tcp** | **udp**} *local-ip local-port global-ip global-port*

Parameters

local-ip	Specifies the private IP address for this static NAPT translation.
local-port	Specifies the L4 source port associated with the private IP address for this static NAPT translation.
global-ip	Specifies the unique public IP address for this static NAPT translation.
global-port	Specifies the L4 translated source port port associated with the unique public IP address for this static NAPT translation.

Defaults

None.

Usage

Packets for the specified protocol from addresses that match the IP address and port for this static entry are translated.

The no version of the command deletes the specified static NAPT translation.

Mode

Router command, Global configuration: **Matrix->Router(config)#**

Example

This example enables a static NAPT translation of inside source addresses for private local address **10.10.10.51** on port **123** destined for and transmitting from unique public address **45.20.10.6** on port **121**:

```
Matrix->Router(config)#ip nat inside source static tcp 10.10.10.51 123 45.20.10.6
121
```

ip nat ftp-control-port

Use this command to specify the NAT FTP control port.

Syntax

ip nat ftp-control-port *port-number*

no ip nat ftp-control-port

Parameters

port-number	Specifies the FTP control port. Default value: **21**.

Downloaded from www.Manualslib.com manuals search engine

Defaults

None.

Mode

Router command, Global configuration: **Matrix->Router(config)#**

Usage

The no version of the command resets the FTP control port to the default value.

Example

This example sets the NAT FTP control port to **22**:

```
Matrix->Router(config)#ip nat ftp-control-port 22
```

ip nat secure-plus

Use this command to enable force flows to block clients on the outside interface from establishing connections directly to the inside interface addresses.

Syntax

ip nat secure-plus

no ip nat secure-plus

Parameters

None

Defaults

None.

Mode

Router command, Global configuration: **Matrix->Router(config)#**

Usage

All flows are translated between outside and inside interfaces when secure-plus is enabled.

The no version of the command disables secure-plus.

Example

This example enables force flows for this router:

```
Matrix->Router(config)#ip nat secure-plus
```


Downloaded from www.Manualslib.com manuals search engine

ip nat translation max-entries

Use this command to configure the maximum number of translation entries.

Syntax

ip nat translation max-entries *number*

no ip nat translation max-entries

Parameters

number	Specifies the maximum number of translation entries allowed for this router. Default value of 32000.

Defaults

None.

Mode

Router command, Global configuration: **Matrix->Router(config)#**

Usage

32,000 entries is currently the maximum value allowed for this command. Certain applications such as NAT, LSNAT, TWCB share the same hardware resource pool of 32,000 on a first come first serve basis. Lowering this value assures resources will be available for other applications.

The no version of the command resets the number of maximum entries to the default value.

Example

This example sets the maximum number of NAT translation entries to **20000**:

```
Matrix->Router(config)#ip nat translation max-entries 20000
```

ip nat translation (timeouts)

Use this command to configure the maximum timeout value in seconds per flow type.

Syntax

ip nat translation {**timeout** | **udp-timeout** | **tcp-timeout** | **icmp-timeout** | **dns-timeout** | **ftp-timeout**} [*seconds*]

no ip nat translation max-entries

Parameters

timeout	Specifies the timeout value applied to dynamic translations. Default: 240 seconds.
udp-timeout	Specifies the timeout value applied to the UDP translations. Default: 240 seconds.
tcp-timeout	Specifies the timeout value applied to the TCP translations. Default: 240 seconds.
icmp-timeout	Specifies the timeout value applied to the ICMP translations. Default: 240 seconds.

Downloaded from www.Manualslib.com manuals search engine

dns-timeout	Specifies the timeout value applied to the DNS translations. Default: 240 seconds.
ftp-timeout	Specifies the timeout value applied to the FTP translations. Default: 240 seconds.
seconds	Specifies the timeout value in seconds.

Defaults

If seconds is not specified, see the parameter table above for the default value.

Mode

Router command, Global configuration: **Matrix->Router(config)#**

Usage

The no version of the command resets the timeouts to the default value.

Example

This example sets the timeout value applied to UDP flows to **400**:

```
Matrix->Router(config)#ip nat translation udp-timeout 400
```

show ip nat translations

Use this command to display active NAT translations.

Syntax

show ip nat translations [**verbose**]

Parameters

None.

Defaults

If **verbose** is not specified, standard output is displayed.

Mode

Router command, Global configuration: **Matrix->Router(config)#**

Examples

This example shows a dynamic NAPT translations display for this router:

```
Matrix->Router(config)#show ip nat translations
Proto  Outside-global          Inside-local             Type     No. of Flows
-------------------------------------------------------------------------------
tcp    81.1.1.1:1024           172.111.1.4:50020        DynOver  14
tcp    81.1.1.1:1025           172.111.1.4:50021        DynOver  2
tcp    81.1.1.1:1026           172.111.1.4:50022        DynOver  10
tcp    81.1.1.1:1027           172.111.1.4:50023        DynOver  2
tcp    81.1.1.1:1029           172.111.1.4:50024        DynOver  3
```


Downloaded from www.Manualslib.com manuals search engine

```
tcp    81.1.1.1:1030           172.111.1.4:50025        DynOver  3
tcp    81.1.1.1:1031           172.111.1.4:50026        DynOver  3
tcp    81.1.1.1:1032           172.111.1.4:50027        DynOver  1
tcp    81.1.1.1:1033           172.111.1.4:50028        DynOver  1
tcp    81.1.1.1:1034           172.111.1.4:50029        DynOver  1
NAT translation count = 10.
```

This example shows a portion of the verbose version of the above example:

```
Matrix->Router(config)#show ip nat translations verbose
Proto  Outside-global          Inside-local             Type     No. of Flows
--------------------------------------------------------------------------------
tcp    81.1.1.1:1024           172.111.1.4:50020        DynOver  14
create 07:39:00 use 00:00:03  service type ftp control
tcp    81.1.1.1:1025           172.111.1.4:50021        DynOver  2
create 07:39:00 use 00:00:03  service type ftp data
tcp    81.1.1.1:1026           172.111.1.4:50022        DynOver  16
create 07:39:02 use 00:00:01  service type ftp data
.
.
.
tcp    84.1.1.1:1024           172.114.1.4:11244        DynOver  4
create 07:39:02 use 00:00:01  service type normal
tcp    84.1.1.1:1027           172.114.1.4:11247        DynOver  4
create 07:39:02 use 00:00:01  service type normal
tcp    84.1.1.1:1028           172.114.1.4:11248        DynOver  1
create 07:39:03 use 00:00:00  service type normal
NAT translation count = 19.
```

show ip nat statistics

Use this command to display NAT translation statistics.

Syntax

show ip nat statistics [**verbose**]

Parameters

If **verbose** is not specified, the standard output is displayed.

Defaults

None.

Mode

Router command, Global configuration: **Matrix->Router(config)#**

Downloaded from www.Manualslib.com manuals search engine

Examples

This example displays the NAT statistics for this router:

```
Matrix->Router(config)#show ip nat statistics

Nat current status:     Active
Nat secure plus:        Disable
Total translations: 953 (0 static, 953 dynamic)

Outside interface: vlan 3000, vlan   21, vlan   20
Inside interface:  vlan 3005, vlan 3004, vlan 3003, vlan 3002, vlan 3001,
                   vlan   15
Created translations:961,  Expired translations:  8, Misses:0
Binding Resource Allocation Failures: 0
```

This example displays a portion of the verbose version of the above example:

```
Matrix->Router(config)#show ip nat statistics verbose

Nat current status:     Active
Nat secure plus:        Disable
Nat maximum allowed translation entries:        32000

All nat timeout value display in minutes:
timeout      udp-timeout  tcp-timeout  icmp-timeout ftp-timeout  dns-timeout
-------------------------------------------------------------------------------
4            4            4            1            4            4

Total translations: 2660 (0 static, 2660 dynamic)

Outside interface: vlan 3000, vlan   21, vlan   20
Inside interface:  vlan 3005, vlan 3004, vlan 3003, vlan 3002, vlan 3001,
                   vlan   15
Created translations:2755,  Expired translations: 95, Misses:0
Binding Resource Allocation Failures: 0

Dynamic mappings:
-- Inside Source
access-list 31 refcount 1008
  pool vlan 3000: netmask 0.0.0.0
  start 81.1.1.1   end 81.1.1.1
  type napt, total addresses 1, allocated 1, max_ports 32000, used_ports 1019 (3
%),
  misses 0
.
.
.
```


Downloaded from www.Manualslib.com manuals search engine

```
access-list 35 refcount 28
  pool vlan 3000: netmask 0.0.0.0
  start 85.1.1.1   end 85.1.1.1
  type napt, total addresses 1, allocated 1, max_ports 32000, used_ports 28 (0%)
,
  misses 0
```

clear ip nat translation

Use this command to clear active dynamic NAT translations.

Syntax

clear ip nat translation

Parameters

None.

Defaults

None.

Mode

Router command, Global configuration: **Matrix->Router(config)#**

Example

This example clears dynamic ip NAT translations for this router:

```
Matrix->Router(config)#clear ip nat translation
```

clear ip nat translation inside (NAT)

Use this command to clear an active simple NAT translation.

Syntax

clear ip nat translation inside *global-ip local-ip*

Parameters

global-ip	Specifies the unique public IP address to clear for this static simple translation.
local-ip	Specifies the private IP address to clear for this static simple translation.

Defaults

None.

Mode

Router command, Global configuration: **Matrix->Router(config)#**

Downloaded from www.Manualslib.com manuals search engine

Usage

This command clears an active translation. Use the **no ip nat inside source static** command to delete a static NAT configuration.

Example

This example clears the simple NAT translation for private address 10.10.10.50 and uniquely public address 45.20.10.5:

```
Matrix->Router(config)#clear ip nat translation inside 45.20.10.5 10.10.10.50
```

clear ip nat translation inside (NAPT)

Use this command to clear an active NAPT translation.

Syntax

clear ip nat translation {**tcp** | **upd**} **inside** *global-ip global-port local-ip local-port*

Parameters

global-ip	Specifies the unique public IP address to clear for this static NAPT translation.
global-port	Specifies the L4 translated source port port associated with the unique public IP address for this static NAPT translation.
local-ip	Specifies the private IP address to clear for this static NAPT translation.
local-port	Specifies the L4 source port associated with the private IP address for this static NAPT translation.

Defaults

None.

Mode

Router command, Global configuration: **Matrix->Router(config)#**

Usage

This command clears an active NAPT translation. Use the **no ip nat inside source static** command to delete a static NAT configuration.

Example

This example clears the TCP NAPT translation for private address 10.10.10.51 and port 123 and uniquely public address 45.20.10.6 and port 123:

```
Matrix->Router(config)#clear ip nat translation tcp inside 45.20.10.6 121
10.10.10.51 123
```


Downloaded from www.Manualslib.com manuals search engine

set router limits (NAT)

Use this command to set NAT configuration limits.

Syntax

```
set router limits {nat-bindings nat-bindings | nat-cache nat-cache |
nat-dynamic-configs nat-dynamic-configs | nat-static-config nat-static-config |
nat-interface-config nat-interface-config | nat-global-addr-cfg
nat-global-addr-cfg | nat-global-port-cfg nat-global-port-cfg}
```

Parameters

nat-bindings *nat-bindings*	(Optional) Specifies the maximum number of NAT bindings for this router. Values range from 500 to 32000. Default value of 32000.
nat-cache *nat-cache*	(Optional) Specifies the maximum NAT cache size for this router. Values range from 100 to 2000. Default value of 2000.
nat-dynamic-configs *nat-dynamic-configs*	(Optional) Specifies the maximum number of dynamic mapping configurations. Values range from 1 to 10. Default value of 10.
nat-static-config *nat-static-config*	(Optional) Specifies the maximum number of NAT static mapping configurations for this router. Values range from 1 - 50. Default value of 50.
nat-interface-config *nat-interface-config*	(Optional) Specifies the maximum number of NAT interface configurations. Values range from 4 - 103. Default value of 103.
nat-global-addr-cfg *nat-global-addr-cfg*	(Optional) Specifies the maximum number of NAT global address configurations for this router. Values range from 1 - 1000. Default value of 1000.
nat-global-port-cfg *nat-global-port-cfg*	(Optional) Specifies the maximum number of NAT global port configurations for this router. Values range from 1 - 32000. Default value of 32000.

Defaults

None.

Mode

Switch Command: **Matrix(rw)->**.

Usage

Bindings and cache use valuable memory resources. By default these setting are set to maximum values. Use this command to free memory resources by limiting the number of bindings and cache size.

The chassis or system must be rebooted for any new change to take effect.

This command must be executed from the switch CLI.

Note: Router limits can also be set in the following contexts:

To set LSNAT router limits see *set router limits (LSNAT)* on page 19-33.

To set TWCB router limits see *set router limits (TWCB)* on page 23-15.

Downloaded from www.Manualslib.com manuals search engine

Example

This example sets the maximum NAT cache size to 1000:

```
Matrix(rw)->set router limits nat-cache 1000
```

show router limits (NAT)

Use this command to display NAT router limit configuration settings.

Syntax

```
show router limits [nat-bindings] [nat-cache] [nat-dynamic-config]
[nat-static-config] [nat-interface-config] [nat-global-addr-cfg]
[nat-global-port-cfg]
```

Parameters

nat-bindings	(Optional) Displays the NAT maximum bindings limit.
nat-cache	(Optional) Displays the NAT cache size limit.
nat-dynamic-configs	(Optional) Displays the NAT dynamic configuration limit.
nat-static-config	(Optional) Displays the NAT static mappings configuration limit.
nat-interface-config	(Optional) Displays the NAT interface configuration limit.
nat-global-addr-cfg	(Optional) Displays the NAT global address configuration limit.
nat-global-port-cfg	(Optional) Displays the NAT global port configuration limit.

Defaults

If no parameters are specified, all router limits are displayed, including TWCB and LSNAT.

Mode

Switch command mode: **Matrix(rw)->**.

Usage

This command must be entered in switch command mode.

Examples

This example displays all router limits for this system:

```
Matrix(su)->show router limits
LSNAT maximum Bindings                      -  32000  (default)
LSNAT Cache size                            -   2000  (default)
LSNAT maximum Configs                       -     50  (default)
NAT maximum Bindings                        -  32000  (default)
NAT Cache size                              -   2000  (default)
NAT maximum dynamic mapping Configs         -     10  (default)
NAT maximum static mapping Configs          -     50  (default)
NAT maximum Interface Configs               -    103  (default)
NAT maximum global address Configs          -   1000  (default)
NAT maximum global port Configs             -  32000  (default)
```


Downloaded from www.Manualslib.com manuals search engine

```
Route Table Limit                          -  12000  (default)
TWCB maximum Bindings                      -  32000  (default)
TWCB Cache size                            -   2000  (default)
TWCB maximum Configs                       -      1  (default)
```

This example displays the NAT cache-size limit for this system:

```
Matrix(su)->show router limits nat-cache
NAT Cache size                             -   2000  (default)
```

clear router limits (NAT)

Use this command to reset NAT router limits to the default values.

Syntax

clear router limits [**nat-bindings**] [**nat-cache**] [**nat-dynamic-config**] [**nat-static-config**] [**nat-interface-config**] [**nat-global-addr-cfg**] [**nat-global-port-cfg**]

Parameters

nat-bindings	(Optional) Specifies the resetting of NAT binding router limits to the default value.
nat-cache	(Optional) Specifies the resetting of NAT cache size router limits to the default value.
nat-dynamic-configs	(Optional) Specifies the resetting the number of NAT dynamic mapping configurations to the default value.
nat-static-config	(Optional) Specifies the resetting the number of NAT static mapping configurations to the default value.
nat-interface-config	(Optional) Specifies the resetting the number of configured NAT VLAN interfaces to the default value.
nat-global-addr-cfg	(Optional) Specifies the resetting the number configurable global addresses to the default value.
nat-global-port-cfg	(Optional) Specifies the resetting the number of configurable global ports to the default value.

Defaults

If no parameters are specified, all router limits are reset, including TWCB, LSNAT and route-table router limits.

Mode

Switch Command: **Matrix(rw)->**.

Usage



Note: Router limits can also be cleared in the following contexts:

To clear LSNAT router limits see *clear router limits (LSNAT)* on page 19-34.

To clear TWCB router limits see *clear router limits (TWCB)* on page 23-17.

If you do not specify a parameter when issuing a **clear router limits** command, router limits for all contexts are reset to the default value.

Downloaded from www.Manualslib.com manuals search engine

Example

This example resets the NAT cache router limits setting to the default value:

```
Matrix(rw)->clear router limits nat-cache
```


Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

19

LSNAT Configuration

This chapter describes the Load Sharing Network Address Translation (LSNAT) configuration set of commands and how to use them.



Router: Unless otherwise noted, the commands covered in this chapter can be executed only when the device is in router mode. For details on how to enable router configuration modes, refer to *Enabling Router Configuration Modes* on page 2-103.



Note: An Enterasys Feature Guide document that contains a complete discussion on LSNAT configuration exists at the following Enterasys web site: http://www.enterasys.com/support/manuals/

Configuring Load Sharing Network Address Translation (LSNAT)

Important Notice

LSNAT is an advanced routing feature that must be enabled with a license key. If you have purchased an advanced license key, and have enabled routing on the device, you must activate your license as described in *Activating Licensed Features* on page 2-58. in order to enable the LSNAT command set. If you wish to purchase an advanced routing license, contact Enterasys Networks Sales.

About LSNAT

As defined in RFC 2391, LSNAT supports network reliability and availability by enabling high traffic servers to load balance. It allows an IP address and port number to become a Virtual IP address and port number (VIP), mapped to many devices. When the VIP is seen as a destination address and destination port number by the LSNAT device, the device traps the packet and then translates the VIP to a real IP address and port combination. It does this by using a selected algorithm for choosing from the group of server addresses, and replaces the VIP with the selected IP address and port number. For outgoing transmissions, the translation is made from the real IP address and port combination to VIP.

LSNAT Configuration Considerations

The following considerations must be taken into account when configuring LSNAT on Enterasys Matrix Series devices:

- On chassis-based systems, only one router per chassis will be allowed to run LSNAT at a given time.
- ALL modules in the chassis must have upgraded memory to 256 MB, and must have an advanced license activated.
- A server farm cannot be shared by different virtual servers.

Downloaded from www.Manualslib.com manuals search engine

- When different virtual server IPs (VIPs) share the same real server in different server farms, the persistence level must be set the same.
- In general, in order to edit or delete a virtual server or real server (serverfarm) configuration, the devices must be first configured "out of service" (**no inservice**) before the changes will be allowed.

Session Persistence

Load balancing clients connect to a *virtual* IP address which, in reality, is redirected to one of several physical servers in a load balancing server farm group. In many web page display applications, a client may have its requests redirected to and serviced by different servers in the group. In certain situations, however, it may be critical that all traffic for the client be directed to the same physical server for the duration of the session—this is the concept of *session persistence*.

When the router receives a new session request from a client for a specific virtual address, the router creates a *binding* between the client (source) IP address/port socket and the (destination) IP address/port socket of the load balancing server selected for this client. Subsequent packets from clients are compared to the list of bindings. If there is a match, the packet is sent to the same server previously selected for this client. If there is not a match, a new binding is created. How the router determines the binding match for session persistence is configured with the **persistence level** command when the virtual server is created.

There are three configurable levels of session persistence:

- **TCP persistence** — a binding is determined by the matching the source IP/port address as well as the virtual destination IP/port address. For example, requests from the client address of 134.141.176.10:1024 to the virtual destination address 207.135.89.16:80 is considered one session and would be directed to the same load balancing server (for example, the server with IP address 10.1.1.1). A request from a different source socket from the same client address to the same virtual destination address would be considered another session and may be directed to a different load balancing server (for example, the server with IP address 10.1.1.2). This is the default level of session persistence.
- **SSL persistence** — a binding is determined by matching the source IP address and the virtual destination IP/port address. Note that requests from *any* source socket with the client IP address are considered part of the same session. For example, requests from the client IP address of 134.141.176.10:1024 or 134.141.176.10:1025 to the virtual destination address 207.135.89.16:80 would be considered one session and would be directed to the same load balancing server (for example, the server with IP address 10.1.1.1).
- **Sticky persistence** — a binding is determined by matching the source and destination IP addresses only. This allows all requests from a client to the same virtual address to be directed to the same load balancing server. For example, both HTTP and HTTPS requests from the client address 134.141.176.10 to the virtual destination address 207.135.89.16 would be directed to the same load balancing server (for example, the server with IP address 10.1.1.1).

Sticky Persistence Configuration Considerations

Sticky persistence functionality provides less security but the most flexible capability for users to load balance all services through a virtual IP address. In addition, this functionality provides better resource usage by the LSNAT router, as well as better performance for the same clients trying to reach the same real servers across different services through a virtual server.

For example, with sticky persistence, HTTP, HTTPS, TELNET and SSH requests from a client (200.1.1.1) to the virtual server address (192.168.1.2) would all be directed to the same real server. The client always goes to the same real server for all the services provided by that server, and it

Downloaded from www.Manualslib.com manuals search engine

would only require the use of one binding hardware resource (instead of one per service per client).

In order to use sticky persistence, the following configuration criteria are required:

- Sticky persistence must be configured for the server farm group (with the **sticky** command) as well as for the virtual server (with the **persistence level** command).
- The real servers in this server farm are to be used for all services. The servers are not allowed to be used with other server farms to support other virtual server services. There is one exception to this rule, described in the next bullet item.
- Sticky means all TCP ports or all UDP ports on the virtual server are supported, but not both. You can create two virtual servers with different IP addresses (one for TCP protocols and one for UDP protocols/ports) and use the same real servers (with different serverfarm names). That way all TCP and UDP ports are supported by the same set of real servers.
- Port 0 in the virtual server has to be used to support this service and is reserved for this purpose.
- The service FTP configuration is not needed for this type of persistence. (See the **virtual** command, "virtual" on page 19-22.)

Configuring Direct Access to Real Servers

When the LSNAT router has been configured with load balancing server farm groups, with real servers and virtual servers configured and "in service," the real servers are protected from direct client access for **all** services. Load sharing clients can only access specific services on the real servers by means of the virtual servers configured to provide those services.

If you also want to provide direct client access to real servers configured as part of a server farm group, there are two mechanisms that can provide direct client access.

The first mechanism, configured within virtual server configuration mode with the **allow accessservers** command, allows you to identify specific clients who can set up connections directly to a real server's IP address, as well as continue to use the virtual server IP address.

The second mechanism, configured in Global configuration mode with the **ip slb allowaccess_all** command, allows all clients to directly access all services provided by real servers, except for those services configured to be accessed by means of a configured virtual server. The real servers are still protected from direct client access for configured services *only*. For example, using this mechanism, if you configured a load balancing server group containing "realserver1" and "realserver2" to provide HTTP service through virtual server "vserver-http," clients can only access the HTTP service on those real servers by means of the "vserver-http" virtual server. However, clients can directly access "realserver1" and "realserver2" for any services *other than* HTTP.

If you combine the two mechanisms, that is, configure **ip slb allowaccess_all** at the Global configuration mode and also configure **allow accessservers** within a virtual server's configuration mode, the clients identified with the **allow accessservers** command will have direct access to the real servers for **all** services (including those provided by a virtual server) and be blocked from using the virtual server. So for example, an "allowed" client can access "realserver1" and "realserver2" directly for all services, including HTTP, but cannot access those servers for HTTP by means of the "vserver-http" virtual server.

Service Verification

UPD port service verification can be enabled on one or more load balancing servers. The firmware accomplishes this by sending a UDP packet with "\r\n" (Carriage Return / Line Feed) as data to

Downloaded from www.Manualslib.com manuals search engine

the UDP port. If the server responds with an ICMP “Port Unreachable” message, it is concluded that the port is not active and the server is reported as “DOWN”. Otherwise, if the server either gets data back from the request to the server or does not get any response at all, it is assumed that the port is active and the server is reported as “UP”. The lack of a response could also be the result of the server itself not being available and could produce an erroneous indication of the server being “UP”. To avoid this when requesting an APP UDP on a UDP port, an ICMP ping is issued first to insure that the server is available before submitting the APP UDP request. This prevents a situation where the UDP port will not return a “Port Unreachable” because of the server itself being down, resulting in LSNAT responding with a false indication that the UDP port is “UP”.

Application Content Verification (ACV)

Application Content Verification (ACV) can be enabled on a port to verify the content of an application on one or more load balancing servers. ACV is a method of ensuring that data coming from your servers remains intact and does not change without your knowledge. ACV can simultaneously protect against server outages, accidental file modification or deletion, and servers whose security have been compromised. By nature, ACV is protocol independent and is designed to work with any type of server that communicates via formatted ASCII text messages, including HTTP, FTP, and SMTP. For ACV verification, you specify the following:

- A string that the router sends to a single server. The string can be a simple HTTP command to get a specific HTML page, or it can be a command to execute a user-defined CGI script that tests the operation of the application.
- The reply that the application on each server sends is back used by the router to validate the content. In the case where a specific HTML page is retrieved, the reply can be a string that appears on the page, such as “OK”. If a CGI script is executed on the server, it should return a specific response (for example, “OK”) that the router can verify.

ACV works by sending a command to your server and searching the response for a certain string. If it finds the string, the server is marked as Up. If the string is not found, the server is marked as Down.

For example, if you sent the following string to your HTTP server, “HEAD / HTTP/1.1\\r\\nHost: www.enterasys.com\\r\\n\\r\\n”, you could expect to get a response of a string returned similar to the following:

```
HTTP/1.1 200 OK
Date: Tue, 11 Dec 2007 20:03:40 GMT
Server: Apache/2.0.40 (Red Hat Linux)
Last-Modified: Wed, 19 Sep 2007 13:56:03 GMT
ETag: “297bc-b52-65f942c0”
Accept-Ranges: bytes
Content-Length: 2898
```

You can search for a reply string of “200 OK” this would result in a successful verification of the service.

Because ACV can search for a string in only the first 255 bytes of the response, in most HTTP cases the response will have to be in the packet's HTTP header (i.e., you will not be able to search for a string contained in the web page itself).

Some protocols such as FTP or SMTP require users to issue a command to close the session after making the request. A **faildetect acv-quit** command allows for the input of the quit string required.

Downloaded from www.Manualslib.com manuals search engine

Purpose

To review and configure Load Sharing Network Address Translation (LSNAT).

LSNAT Configuration Task List and Commands

Table 19-1 lists the mandatory and optional tasks and commands for configuring LSNAT on the Enterasys Matrix Series device. Commands are described in the associated sections as shown.

Table 19-1 LSNAT Configuration Task List and Commands

Task	Use these commands...
Configure a server farm:	
(Optional) Display the server farm configuration.	show ip slb serverfarms (“show ip slb serverfarms” on page 19-6)
(Optional) Define an FTP control port.	ip slb ftpctrlport (“ip slb ftpctrlport” on page 19-7)
Specify a server farm name.	ip slb serverfarm (“ip slb serverfarm” on page 19-8)
Specify a real server as a member of the server farm.	real (“real” on page 19-8)
(Optional) Specify a load balancing algorithm.	predictor (“predictor” on page 19-9)
(Optional) Configure this server farm to use sticky session persistence. (See “Sticky Persistence Configuration Considerations” on page 19-2 for more information.)	sticky (“sticky” on page 19-10)
Configure a real server:	
(Optional) Display the real server configuration.	show ip slb reals (“show ip slb reals” on page 19-10)
Enable a real server for service.	inservice (“inservice (real server)” on page 19-13)
(Optional) Configure real server error handling.	faildetect (“faildetect (real server)” on page 19-13)
(Optional) Set the ACV command string to send to the server application port.	faildetect acv-command (“faildetect acv-command” on page 19-15)
(Optional) Set the expected validation ACV reply string from the server application port.	faildetect acv-reply (“faildetect acv-reply” on page 19-16)
(Optional) Issue a command to close the session.	faildetect acv-quit (“faildetect acv-quit” on page 19-16)
(Optional) Set an exact acv-reply string index when the file is not known to the user.	faildetect read-till-index (“faildetect read-till-index” on page 19-17)
(Optional) Limit active connections to the real server.	maxconns (“maxconns” on page 19-18)
(Optional) Specify a weight load number for the real server.	weight (“weight” on page 19-18)
Configure a virtual server:	
(Optional) Display the virtual server configuration.	show ip slb vservers (“show ip slb vservers” on page 19-19)
Specify a virtual server name.	ip slb vserver (“ip slb vserver” on page 19-21)

Downloaded from www.Manualslib.com manuals search engine

Table 19-1 LSNAT Configuration Task List and Commands (continued)

Task	Use these commands...
Associate a virtual server with a server farm.	serverfarm (“serverfarm (Virtual Server)” on page 19-22)
Configure a virtual server IP address (VIP).	virtual (“virtual” on page 19-22)
Enable a virtual server for service.	inservice (“inservice (virtual server)” on page 19-24)
(Optional) Restrict access to specific virtual server clients.	client (“client” on page 19-24)
(Optional) Specify the type of session persistence and timeout. Default is TCP. (See “Session Persistence” on page 19-2 for more information.)	persistence level (“persistence level” on page 19-25)
(Optional) Allow specific clients direct access to a real server without using LSNAT.	allow accessservers (“allow accessservers” on page 19-27)
Configure global direct access:	
(Optional) Allow all clients to directly access all services provided by real servers, EXCEPT FOR those services configured to be accessed through a configured virtual server. (See “Configuring Direct Access to Real Servers” on page 19-3 for more information.)	ip slb allowaccess_all (“ip slb allowaccess_all” on page 19-28)
Display or clear server load balancing connections and statistics:	
(Optional) Display server load balancing connections and statistics.	show ip slb conns (“show ip slb conns” on page 19-29)
	show ip slb stats (“show ip slb stats” on page 19-30)
(Optional) Display SLB active sticky persistence connections.	show ip slb sticky (“show ip slb sticky” on page 19-31)
(Optional) Clear server load balancing connections or statistics.	clear ip slb (“clear ip slb” on page 19-32)
Display and set chassis-based LSNAT limits:	
(Optional) Display and set chassis-based LSNAT address translation limits, from the switch CLI. **Note:** These commands must be executed from the switch CLI.	show router limits (“show router limits (LSNAT)” on page 19-32)
	set router limits (“set router limits (LSNAT)” on page 19-33)
	clear router limits (“clear router limits (LSNAT)” on page 19-34)

show ip slb serverfarms

Use this command to display server load balancing server farm information.

Syntax

show ip slb serverfarms [**detail** | *serverfarmname* [**detail**]]

Downloaded from www.Manualslib.com manuals search engine

Parameters

detail	(Optional) Displays detailed output for a specific server farm or for all configured server farms.
serverfarmname	(Optional) Specifies a server farm name for which to display information.

Defaults

If no parameter is specified, summary information for all configured server farms will be displayed.

Mode

Router command, Any router mode.

Example

This example shows how to display LSNAT server farm summary information:

```
Matrix Router(config)#>show ip slb serverfarms
server-farm              predictor         status      rserver   rserver
-------------------------------------------------------------------------------
matrix                   LEASTCONNECTION   ACTIVE            2         2
ftpserver                ROUNDROBIN        ACTIVE            2         2
ten                      ROUNDROBIN        ACTIVE            3         3
big                      ROUNDROBIN        ACTIVE            1         1
```

ip slb ftpctrlport

Use this command to specify an FTP control port for load balancing functionality. By default, this is port 21.

Syntax

ip slb ftpctrlport *port-number*

no ip slb ftpctrlport

Parameters

port-number	Specifies an FTP port number

Defaults

None.

Mode

Router command, Global configuration mode: **Matrix>Router(config)#**

Usage

The “no” form of this command resets the FTP control port to 21.

Downloaded from www.Manualslib.com manuals search engine

Example

This example shows how to specify port 46 as the FTP control port for server load balancing:

```
Matrix>Router(config)#ip slb ftpctrlport 46
```

ip slb serverfarm

Use this command to identify an LSNAT server farm and enable server load balancing (SLB) server farm configuration mode.

Syntax

ip slb serverfarm *serverfarmname*

no ip slb serverfarm *serverfarmname*

Parameters

serverfarmname	Specifies a server farm name.

Defaults

None.

Mode

Router command, Global configuration mode: **Matrix>Router(config)#**

Usage

The "no" form of this command deletes the server farm from the LSNAT configuration.

Example

This example shows how to identify a server farm named "httpserver" and enable configuration mode for that server farm:

```
Matrix>Router(config)#ip slb serverfarm httpserver
Matrix>Router(config-slb-sfarm)#
```

real

Use this command to add a real LSNAT server to a server farm and to enable LSNAT real server configuration mode.

Syntax

real *ip-address* **port** *number*

no real *ip-address*

Parameters

ip-address	Specifies a server IP address.
port *number*	Specifies a port number for this server.

Downloaded from www.Manualslib.com manuals search engine

Defaults

None.

Mode

Router command, SLB Server Farm Configuration mode: **Matrix>Router(config-slb-sfarm)#**

Usage

For backwards compatibility, entering a port number is optional for TCP session persistence only. However, the recommended procedure is to *always* configure a port number for a real server.

All real servers in the same server farm should be configured to use the same port.

The "no" form of this command removes the server from the server farm.

Example

This example shows how to add a real server 10.1.2.3 to the server farm named "httpserver" and to configure the port number to be used for the service provided by this server:

```
Matrix>Router(config)#ip slb serverfarm httpserver
Matrix>Router(config-slb-sfarm)#real 10.1.2.3 port 80
Matrix>Router(config-slb-real)#
```

predictor

Use this command to specify which load balancing algorithm to use for selecting a real server in an LSNAT server farm.

Syntax

predictor [**roundrobin** | **leastconns**]

no predictor

Parameters

roundrobin | **leastconns**	(Optional) Specifies Round Robin or Least Connections as the selection algorithm.

Defaults

If not specified, Round Robin will be used as the selection algorithm.

Mode

Router command, SLB Server Farm Configuration mode: **Matrix>Router(config-slb-sfarm)#**

Usage

The "no" form of this command resets the selection algorithm to Round Robin.

Downloaded from www.Manualslib.com manuals search engine

Example

This example shows how to specify Least Connections as the server selection algorithm for the "httpserver" server farm:

```
Matrix>Router(config)#ip slb serverfarm httpserver
Matrix>Router(config-slb-sfarm)#predictor leastconns
```

sticky

Use this command to configure sticky session persistence for this server farm.

Syntax

sticky

no sticky

Parameters

None.

Defaults

None.

Mode

Router command, SLB Server Farm Configuration mode: **Matrix>Router(config-slb-sfarm)#**

Usage

See "Sticky Persistence Configuration Considerations" on page 19-2 for more information.

This command is used in conjunction with the **persistence level sticky** command described in "persistence level" on page 19-25.

The "no" form of this command removes this server farm using persistence sticky.

Example

This example shows how to set sticky persistence for the "lsnat" server farm:

```
Matrix>Router(config)#ip slb serverfarm lsnat
Matrix>Router(config-slb-sfarm)#sticky
```

show ip slb reals

Use this command to display information about the real servers.

Syntax

show ip slb reals [**detail** | **serverfarm** *serverfarmname* [**detail**]]

Downloaded from www.Manualslib.com manuals search engine

Parameters

detail	(Optional) Displays detailed output for a specific server farm or for all configured server farms.
serverfarm *serverfarmname*	(Optional) Specifies a server farm name for which to display information.

Defaults

If no parameter is specified, summary information about all configured server farms will be displayed.

Mode

Router command, Any router mode.

Example

This example shows how to display detailed information for real servers in the "ten" server farm:

```
Matrix Router(config)#>Router>show ip slb reals serverfarm ten detail
Server Farm : ten
        Real Server IP : 10.3.0.3
                Real Server Port : 80
                Fail Detect Ping Retries:4 Ping Interval : 200
                Fail Detect App Retries:4 App Interval : 15
                Fail Detect Type : ping
                Current Connections on this real server: 0
                Current state of this real server: UP
                Maximum Connections : Unlimited
                Real Server Weight : 3
                InService

        Real Server IP : 10.3.0.2
                Real Server Port : 80
                Fail Detect Ping Retries:4 Ping Interval : 200
                Fail Detect App Retries:4 App Interval : 15
                Fail Detect Type : ping
                Current Connections on this real server: 0
                Current state of this real server: UP
                Maximum Connections : 350
                Real Server Weight : 2
                InService

        Real Server IP : 10.3.0.1
                Real Server Port : 80
                Fail Detect Ping Retries:4 Ping Interval : 200
                Fail Detect App Retries:4 App Interval : 15
                Fail Detect Type : ping
```


Downloaded from www.Manualslib.com manuals search engine

```
                Current Connections on this real server: 0
                Current state of this real server: UP
                Maximum Connections : Unlimited
                Real Server Weight : 1
                InService

real-serv-ip:port     server-farm               type ins stat wgt maxcon  conns
-------------------------------------------------------------------------------
192.169.1.11:23       matrix                    both  IS  UP   1   N\A     0
192.169.1.10:23       matrix                    ping  IS  UP   1   2       0
192.169.2.14:21       ftpserver                 ping  IS  UP   1   N\A     0
192.169.2.13:21       ftpserver                  app  IS  UP   1   N\A     0
10.3.0.3:80           ten                       none  IS  UP   3   N\A     0
10.3.0.2:80           ten                       none  IS  UP   2   350     0
10.3.0.1:80           ten                       none  IS  UP   1   N\A     0
192.169.2.13:0        big                       ping  IS  UP   1   N\A     0
```

Table 19-2 provides an explanation of the detailed command output.

Table 19-2 show ip slb reals Output Details

Output...	What it displays...
Server Farm	Name of the server farm associated with this server. Assigned using the **ip slb serverfarm** command as described in "ip slb serverfarm" on page 19-8.
Real Server IP	Address of the real server(s) assigned to this server farm. Assigned using the **real** command as described in "real" on page 19-8.
Real Server Port	Port number assigned to this server.
Fail Detect Ping/App Retries	Number of failure detection ping, UDP application, or TCP application retries that will result in an error condition on this server. Defaults can be changed using the **faildetect** command as described in "faildetect (real server)" on page 19-13.
Fail Detect Type	Whether or not the failure detection mechanism is ICMP ping, UDP application, TCP application, both, or none. Assigned using the **faildetect** command as described in "faildetect (real server)" on page 19-13.
Current Connections	Number of active connections on this server.
Current State	Operational state of this server.
Maximum Connections	Number of maximum connections allowed on this server. Default of unlimited can be changed using the **maxconns** command as described in "maxconns" on page 19-18.
Real Server Weight	Weight load number of the real server. Default of 1 can be changed using the **weight** command as described in "weight" on page 19-18.
In Service / Not In Service	Whether or not this server is enabled (using the **inservice** command as described in "inservice (real server)" on page 19-13).

Downloaded from www.Manualslib.com manuals search engine

inservice (real server)

Use this command to enable a real LSNAT server.

Syntax

inservice

no inservice

Parameters

None.

Defaults

None.

Mode

Router command, SLB Real Server Configuration mode: **Matrix>Router(config-slb-real)#**

Usage

The "no" form of this command removes the real server from service.

Example

This example shows how to enable the real server IP 10.1.2.3 in the "httpserver" server farm:

```
Matrix>Router(config)#ip slb serverfarm httpserver
Matrix>Router(config-slb-sfarm)#real 10.1.2.3 port 80
Matrix>Router(config-slb-real)#inservice
```

faildetect (real server)

Use this command to configure which method (type) is used to detect whether an LSNAT server is up or down.

Syntax

faildetect {**type** {**both** | **ping** | **app** [**upd**] | **acv** [**udp**]}} | **ping-int** *seconds* **ping-retries** *number* | **app-int** *seconds* **app-retries** *number*

no faildetect

Downloaded from www.Manualslib.com manuals search engine

Parameters

type both | **ping** | **app** [**upd**] | **acv** [**udp**]	Specifies that the failure detection mechanism will be ping, TCP or UDP application, ACV, or that both application TCP and ping methods will be used as follows: • **acv** - Set or reset auto command verification as the fail detect mechanism • **app** - Set or reset application port monitoring as the fail detect mechanism • **both** - Set or reset ping and application TCP as the fail detect mechanisms • **ping** - Set or reset ping as the fail detect mechanism The ping type determines whether of not a real server in a server farm will be pinged for connectivity before being selected as a potential LSNAT server. Application and ACV default to TCP. You can optionally specify UDP for each type.
ping-int *seconds*	Specifies an ICMP ping failure detection interval in seconds. Valid values are **1** - **200**. Default is 5 seconds.
ping-retries *number*	Specifies the number of times an ICMP ping failure will result in a retry. Valid values are **1** - **200**. Default is 4.
app-int *seconds*	Specifies an application failure detection interval in seconds. Default is 15 seconds.
app-retries *number*	Specifies the number of times a TCP application failure will result in a retrial. Default is 3.

Defaults

If not specified, **ping** will be chosen as the fail detection type. Unless the UDP option is specified, app defaults to TCP.

Mode

Router command, SLB Real Server Configuration mode: **Matrix>Router(config-slb-real)#**

Usage

The “no” form of this command resets the fail detection configuration parameters to default values.

Examples

This example shows how to set the ping interval to 10 seconds and the retry number to 6 for the real server at IP 10.1.2.3 in the “httpserver” server farm:

```
Matrix>Router(config)#ip slb serverfarm httpserver
Matrix>Router(config-slb-sfarm)#real 10.1.2.3 port 80
Matrix>Router(config-slb-real)#faildetect ping-int 10 ping-retries 6
Matrix>Router(config-slb-real)#inservice
```

This example sets the app type to UPD for the real server at IP 10.1.2.4 in the “SF-UDP” server farm:

```
Matrix>Router(config)#ip slb serverfarm SF-UPD
Matrix>Router(config-slb-sfarm)#real 10.1.2.4 port 7
```


Downloaded from www.Manualslib.com manuals search engine

```
Matrix>Router(config-slb-real)#faildetect type app udp
Matrix>Router(config-slb-real)#inservice
```

This example sets the ACV protocol to TCP for the real server at IP 10.1.2.5 in the “SF-TCP” server farm:

```
Matrix>Router(config)#ip slb serverfarm SF-TCP
Matrix>Router(config-slb-sfarm)#real 10.1.2.5 port 80
Matrix>Router(config-slb-real)#faildetect type acv
Matrix>Router(config-slb-real)#inservice
```

faildetect acv-command

Use this command to set the command string to send to the server application port.

Syntax

faildetect acv-command *“command-string”*

Parameters

command-string	Specifies the command string sent to the application port of the server.

Defaults

None.

Mode

Router command, SLB Real Server Configuration mode: **Matrix>Router(config-slb-real)#**

Usage

The ACV *command-string* is required when the faildetect type is ACV. This is the command that is sent to the application port of the server and for which it's reply will be validated against the ACV *reply-string* specified in the command “faildetect acv-reply” on page 19-16.

A Carriage Return / Line Feed character “\\r\\n” should be included in the *command-string* if it is required by the server. Carriage Returns & Line Feeds are control characters and require a double backslash “\\” to be treated as control characters. i.e. '\\r' is a Carriage Return and '\\n' is a Line Feed.

Example

This example sends the command string “HEAD / HTTP/1.1\\r\\nHost: www.enterasys.com\\r\\n\\r\\n” to the server application port 7:

```
Matrix>Router(config)#ip slb serverfarm SF-UPD
Matrix>Router(config-slb-sfarm)#real 10.1.2.4 port 7
Matrix>Router(config-slb-real)#faildetect type app udp
Matrix>Router(config-slb-real)#faildetect acv-command “HEAD / HTTP/1.1\\r\\nHost:
www.enterasys.com\\r\\n\\r\\n”
Matrix>Router(config-slb-real)#inservice
```


Downloaded from www.Manualslib.com manuals search engine

faildetect acv-reply

Use this command to set the expected validation ACV reply string from the server application port.

Syntax

faildetect acv-reply *"reply-string"*

Parameters

reply-string	Specifies the expected reply returned from the server to the command string sent to the server.

Defaults

None.

Mode

Router command, SLB Real Server Configuration mode: **Matrix>Router(config-slb-real)#**

Usage

The reply to the ACV *command-string* is validated against the ACV *reply-string* specified in this command.

Example

This example expects to receive "200 OK" in reply to the command string sent to the server application port 7:

```
Matrix>Router(config)#ip slb serverfarm SF-UPD
Matrix>Router(config-slb-sfarm)#real 10.1.2.4 port 7
Matrix>Router(config-slb-real)#faildetect type app udp
Matrix>Router(config-slb-real)#faildetect acv-reply "200 OK"
Matrix>Router(config-slb-real)#inservice
```

faildetect acv-quit

Use this command when the protocol requires the user to issue a command to close the session.

Syntax

faildetect acv-quit *"quit-string"*

Parameters

quit-string	Specifies the quit string expected by the ACV session.

Defaults

None.

Mode

Router command, SLB Real Server Configuration mode: **Matrix>Router(config-slb-real)#**

Downloaded from www.Manualslib.com manuals search engine

Usage

A Carriage Return / Line Feed character "\\r\\n" is appended to the quit string when it is sent to the server. It is not necessary to put a CR or LF in your acv-quit string. For example, when working with FTP, use "BYE" rather than "BYE\\r\\n."

Example

This example provides the quit string **quit** for the port 25 session on the "SF-UDP" server farm:

```
Matrix>Router(config)#ip slb serverfarm SF-UPD
Matrix>Router(config-slb-sfarm)#real 10.1.2.4 port 25
Matrix>Router(config-slb-real)#faildetect acv-command "noop\\r\\n" acv-reply "OK"
Matrix>Router(config-slb-real)#faildetect acv-quit "quit"
Matrix>Router(config-slb-real)#inservice
```

faildetect read-till-index

Provides for the setting of an exact acv-reply string index when the file is not known to the user.

Syntax

faildetect read-till-index *index-number*

Parameters

index-number	Specifies the index to read to in the reply search range. Valid values: **1**-**255**. Default: **255**.

Defaults

None.

Mode

Router command, SLB Real Server Configuration mode: **Matrix>Router(config-slb-real)#**

Usage

The router will search from the beginning of the file up to the **read-till-index** number of characters for the start of the acv-reply string.

Example

This example sets the read to index for this search to 100 characters:

```
Matrix>Router(config)#ip slb serverfarm SF-UPD
Matrix>Router(config-slb-sfarm)#real 10.1.2.4 port 25
Matrix>Router(config-slb-real)#faildetect acv-command "noop\\r\\n" acv-reply "OK"
Matrix>Router(config-slb-real)#faildetect read-till-index 100
Matrix>Router(config-slb-real)#inservice
```


Downloaded from www.Manualslib.com manuals search engine

maxconns

Use this command to limit the number of connections to a real LSNAT server.

Syntax

maxconns *maximum-number*

no maxconns

Parameters

maximum-number	Specifies the maximum number of connections allowed. The default condition is unlimited number of connections.

Defaults

None.

Mode

Router command, SLB Real Server Configuration mode: **Matrix>Router(config-slb-real)#**

Usage

The "no" form of this command removes the limit of connections to the server.

Example

This example shows how to limit the number of connections to 20 on the real server at IP 10.1.2.3 in the "httpserver" server farm:

```
Matrix>Router(config)#ip slb serverfarm httpserver
Matrix>Router(config-slb-sfarm)#real 10.1.2.3 port 80
Matrix>Router(config-slb-real)#faildetect ping-int 10 ping-retries 6
Matrix>Router(config-slb-real)#maxconns 20
Matrix>Router(config-slb-real)#inservice
```

weight

Use this command to specify the weight load number of a real server that is a member of an LSNAT server farm.

Syntax

weight *weight-number*

no weight *weight-number*

Parameters

weight-number	Specifies the weight load number. Valid values are 1-255.

Defaults

None.

Downloaded from www.Manualslib.com manuals search engine

Mode

Router command, SLB Real Server Configuration mode: **Matrix>Router(config-slb-real)#**

Usage

The "no" form of this command resets the weight load number to the default value of 1.

Example

This example shows how to set the weight load number to 100 on the real server at IP 10.1.2.3 in the "httpserver" server farm:

```
Matrix>Router(config)#ip slb serverfarm httpserver
Matrix>Router(config-slb-sfarm)#real 10.1.2.3 port 80
Matrix>Router(config-slb-real)#faildetect ping-int 10 ping-retries 6
Matrix>Router(config-slb-real)#maxconns 20
Matrix>Router(config-slb-real)#weight 100
Matrix>Router(config-slb-real)#inservice
```

show ip slb vservers

Use this command to display server load balancing virtual server information.

Syntax

show ip slb vservers [**detail** | *virtserver-name* [**detail**]]

Parameters

detail	(Optional) Displays detailed output for a specific virtual server or for all configured virtual servers.
virtserver-name	(Optional) Specifies a virtual server name for which to display information.

Defaults

If *virtserver-name* is not entered, information about all configured virtual servers will be displayed.

If **detail** is not specified, summary information will be displayed.

Mode

Router command, Any router mode.

Examples

This example shows how to display summary information about all LSNAT virtual servers:

```
Matrix Router(config)#>show ip slb vservers
                                vserv              persistence     service
virt-serv       vserv-ip-addr   port  server-farm  type  level ins   name
-------------------------------------------------------------------------------
telnet          192.169.10.1    23    matrix       STICKY 200   IS
wftpd           192.169.10.3    21    ftpserver    SSL   240    IS
```


Downloaded from www.Manualslib.com manuals search engine

```
five             3.3.3.3          80    ten          TCP   41     IS
test             192.169.10.88    80    big          TCP   240    IS    ftp
```

This example shows how to display detailed information about the "test" virtual server:

```
Matrix Router(config)#>show ip slb vservers test detail
Virtual Server : test
Virtual Server IP : 192.168.2.2
Port : 23
Server Farm : test1
Persistence Type : TCP Level : 240
Virtual Server Protocol Type : TCP
In Service
Service Name :

client(s) allowed to use the virtual server(s)
----------------------------------------------
Virtual Server : test
Client IP/Mask : 169.254.1.1/255.255.255.0

client(s) allowed direct access to the real server(s)
-----------------------------------------------------
Virtual Server : test
Start IP to End IP : 169.254.1.1 to 169.254.1.9
```

Table 19-3 provides an explanation of the detailed command output.

Table 19-3 show ip slb vservers Output Details

Output...	What it displays...
Virtual Server	Name of the virtual server. Assigned using the **ip slb vserver** command as described in "ip slb vserver" on page 19-21.
Virtual Server IP	Address of the virtual server. Assigned with the **virtual** command as described in "virtual" on page 19-22.
Port	TCP or UDP port number assigned to this server.
Server Farm	Name of the server farm associated with this server. Assigned with the **serverfarm** command as described in "serverfarm (Virtual Server)" on page 19-22.
Persistence Type	Type of binding used and time limit to allow clients to bind to an LSNAT virtual server. Set using the **persistence level** command as described in "persistence level" on page 19-25.
Virtual Server Protocol Type	Whether this virtual server is using the TCP or UDP protocol.
In Service	Whether or not this virtual server is enabled (using the **inservice** command as described in "inservice (virtual server)" on page 19-24).
Service Name	Whether or not the service named can also be accessed through this virtual server IP address. Configured using the **virtual** command as described in "virtual" on page 19-22. Note that currently only FTP is supported.

Downloaded from www.Manualslib.com manuals search engine

Table 19-3 show ip slb vservers Output Details (continued)

Output...	What it displays...
client(s) allowed to use the virtual server(s)	Clients with permission to access this server. Set with the **client** command as described in “client” on page 19-24.
client(s) allowed direct access to the real server(s)	Clients with permission to access this server without LSNAT translation. Set with the **allow accessservers** command as described in “allow accessservers” on page 19-27.

ip slb vserver

Use this command to identify an LSNAT virtual server and to access or enable the virtual server load balance (SLB) configuration mode.

Syntax

ip slb vserver *vserver-name*

no ip slb vserver *vserver-name*

Parameters

vserver-name	Specifies a virtual server name.

Defaults

None.

Mode

Router command, Global configuration mode: **Matrix>Router(config)#**

Usage

The “no” form of this command deletes the virtual server from the LSNAT configuration.

Example

This example shows how to identify a virtual server named “virtual-http” and enable configuration mode for that virtual server. Note that this example also includes the configuration of the server farm to which this virtual server will be associated.

```
Matrix>Router(config)#ip slb serverfarm httpserver
Matrix>Router(config-slb-sfarm)#real 10.1.2.1 port 80
Matrix>Router(config-slb-real)#inservice
Matrix>Router(config-slb-real)#exit
Matrix>Router(config-slb-sfarm)#real 10.1.2.3 port 80
Matrix>Router(config-slb-real)#inservice
Matrix>Router(config-slb-real)#exit
Matrix>Router(config-slb-sfarm)#exit
Matrix>Router(config)#ip slb vserver virtual-http
Matrix>Router(config-slb-vserver)#
```


Downloaded from www.Manualslib.com manuals search engine

serverfarm (Virtual Server)

Use this command to associate a virtual server with an LSNAT server farm.

Syntax

serverfarm *serverfarm-name*

no serverfarm *serverfarm-name*

Parameters

serverfarm-name	Specifies a server farm name. Must be previously configured with the **ip slb serverfarm** command as described in "ip slb serverfarm" on page 19-8.

Defaults

None.

Mode

Router command, SLB Virtual Server Configuration mode: **Matrix>Router(config-slb-vserver)#**

Usage

The "no" form of this command removes the virtual server association.

Example

This example shows how to associate the virtual server named "virtual-http" to the "httpserver" server farm:

```
Matrix>Router(config)#ip slb serverfarm httpserver
Matrix>Router(config-slb-sfarm)#real 10.1.2.1 port 80
Matrix>Router(config-slb-real)#inservice
Matrix>Router(config-slb-real)#exit
Matrix>Router(config-slb-sfarm)#real 10.1.2.3 port 80
Matrix>Router(config-slb-real)#inservice
Matrix>Router(config-slb-real)#exit
Matrix>Router(config-slb-sfarm)#exit
Matrix>Router(config)#ip slb vserver virtual-http
Matrix>Router(config-slb-vserver)#serverfarm httpserver
```

virtual

Use this command to configure a virtual server IP address.

Syntax

virtual *ip-address* {**tcp** | **udp**} *port* [**service** *service-name*]

no virtual *ip-address*

Downloaded from www.Manualslib.com manuals search engine

Parameters

ip-address	Specifies an IP address for the virtual server.
tcp | **udp**	Specifies TCP or UDP as the protocol used by the virtual server.
port	Specifies a TCP or UDP port number (0 through 65535) or port name to be used by this virtual server. Specifying 0 indicates all ports can be used by this virtual server, and should be used only with sticky session persistence configuration. See "Sticky Persistence Configuration Considerations" on page 19-2 The following port name keywords may be used: **ftp** — File Transfer Protocol, port 21 **telnet** — Telnet, port 23 **www** — World Wide Web, port 80
service *service-name*	(Optional) Specifies the service to be accessed through this virtual server IP address when TCP is specified. Currently, only **ftp** may be specified.

Defaults

If a TCP **service** name is not specified, none will be applied.

Mode

Router command, SLB Virtual Server Configuration mode: **Matrix>Router(config-slb-vserver)#**

Usage

If sticky session persistence is configured with the **persistence level** command ("persistence level" on page 19-25), the service parameter is not needed.

The "no" form of this command clears the virtual server configuration.

Example

This example shows how to set the IP address and TCP port for the "virtual-http" virtual server:

```
Matrix>Router(config)#ip slb serverfarm httpserver
Matrix>Router(config-slb-sfarm)#real 10.1.2.1 port 80
Matrix>Router(config-slb-real)#inservice
Matrix>Router(config-slb-real)#exit
Matrix>Router(config-slb-sfarm)#real 10.1.2.3 port 80
Matrix>Router(config-slb-real)#inservice
Matrix>Router(config-slb-real)#exit
Matrix>Router(config-slb-sfarm)#exit
Matrix>Router(config)#ip slb vserver virtual-http
Matrix>Router(config-slb-vserver)#serverfarm httpserver
Matrix>Router(config-slb-vserver)#virtual 10.1.4.5 tcp www
```


Downloaded from www.Manualslib.com manuals search engine

inservice (virtual server)

Use this command to enable a virtual LSNAT server.

Syntax

inservice

no inservice

Parameters

None.

Defaults

None.

Mode

Router command, SLB Virtual Server Configuration mode: **Matrix>Router(config-slb-vserver)#**

Usage

The "no" form of this command removes the virtual server from service.

Example

This example shows how to enable virtual server named "virtual-http":

```
Matrix>Router(config)#ip slb serverfarm httpserver
Matrix>Router(config-slb-sfarm)#real 10.1.2.1 port 80
Matrix>Router(config-slb-real)#inservice
Matrix>Router(config-slb-real)#exit
Matrix>Router(config-slb-sfarm)#real 10.1.2.3 port 80
Matrix>Router(config-slb-real)#inservice
Matrix>Router(config-slb-real)#exit
Matrix>Router(config-slb-sfarm)#exit
Matrix>Router(config)#ip slb vserver virtual-http
Matrix>Router(config-slb-vserver)#serverfarm httpserver
Matrix>Router(config-slb-vserver)#virtual 10.1.4.5 tcp www
Matrix>Router(config-slb-vserver)#inservice
```

client

Use this command to allow a specific client to use a virtual server.

Syntax

client [*ip-address network-mask*]

no client [*ip-address network-mask*]

Downloaded from www.Manualslib.com manuals search engine

Parameters

ip-address	(Optional) Specifies a client's IP address.
network-mask	(Optional) Specifies a client's network mask.

Defaults

None.

Mode

Router command, SLB Virtual Server Configuration mode: **Matrix>Router(config-slb-vserver)#**

Usage

If no clients are specified with this command, all clients will be allowed to use a virtual server.

The "no" form of this command removes permission for a client to use the virtual server.

Example

This example shows how to allow a client at 100.12.22.42 255.255.255.0 to use the virtual server named "virtual-lsnat":

```
Matrix>Router(config)#ip slb vserver virtual-lsnat
Matrix>Router(config-slb-vserver)#client 100.12.22.42 255.255.255.0
```

persistence level

Use this command to set the type of binding used and the time limit to allow clients to remain bound to an LSNAT virtual server.

Syntax

persistence level [**tcp** | **ssl** | **sticky**] *timeperiod*

no persistence level {**tcp** | **ssl** | **sticky**}

Downloaded from www.Manualslib.com manuals search engine

Parameters

tcp | **ssl** | **sticky**	(Optional) Specifies the type of binding that is used to connect a client to a server. TCP is the default. **TCP** will bind based on four fields within the packets (source IP address, destination IP address, source port, and destination port). **SSL** will bind based on source IP address, destination IP address, and destination port. **Sticky** will configure sticky persistence based on source IP address, destination IP address. This parameter is used in conjunction with the **sticky** command described in "sticky" on page 19-10
timeperiod	Specifies the time (in seconds) after which a binding connection between clients and the virtual server will be removed. Default timeout values are: TCP: 240 seconds SSL: 7200 seconds Sticky: 7200 seconds

Defaults

If not specified, persistence level is set to TCP.

Mode

Router command, SLB Virtual Server Configuration mode: **Matrix>Router(config-slb-vserver)#**

Usage

See "Session Persistence" on page 19-2 for more information.

The "no" form of this command resets the timeout to the default of 240 seconds for TCP, 7200 seconds for SSL, and 7200 seconds for Sticky.

Examples

This example shows how to set the TCP session persistence timeout to 360 seconds on the virtual server named "virtual-http":

```
Matrix>Router(config)#ip slb serverfarm httpserver
Matrix>Router(config-slb-sfarm)#real 10.1.2.1 port 80
Matrix>Router(config-slb-real)#inservice
Matrix>Router(config-slb-real)#exit
Matrix>Router(config-slb-sfarm)#real 10.1.2.3 port 80
Matrix>Router(config-slb-real)#inservice
Matrix>Router(config-slb-real)#exit
Matrix>Router(config-slb-sfarm)#exit
Matrix>Router(config)#ip slb vserver virtual-http
Matrix>Router(config-slb-vserver)#serverfarm httpserver
Matrix>Router(config-slb-vserver)#virtual 10.1.4.5 tcp www
Matrix>Router(config-slb-vserver)#persistence level tcp 360
Matrix>Router(config-slb-vserver)#inservice
```


Downloaded from www.Manualslib.com manuals search engine

This example shows how to use sticky session persistence, in conjunction with the **sticky** server farm parameter.

```
Matrix>Router(config)#ip slb serverfarm lsnat
Matrix>Router(config-slb-sfarm)#sticky
Matrix>Router(config-slb-sfarm)#real 10.1.2.10 port 80
Matrix>Router(config-slb-real)#inservice
Matrix>Router(config-slb-real)#exit
Matrix>Router(config-slb-sfarm)#real 10.1.2.11 port 80
Matrix>Router(config-slb-real)#inservice
Matrix>Router(config-slb-real)#exit
Matrix>Router(config-slb-sfarm)#exit
Matrix>Router(config)#ip slb vserver virtual-lsnat
Matrix>Router(config-slb-vserver)#serverfarm lsnat
Matrix>Router(config-slb-vserver)#virtual 10.1.4.5 tcp 0
Matrix>Router(config-slb-vserver)#persistence level sticky
Matrix>Router(config-slb-vserver)#inservice
```

allow accessservers

Use this command to allow specific clients to access the load balancing real servers in a particular LSNAT server farm without address translation.

Syntax

allow accessservers *client-ip-start client-ip-end*

no allow accessservers *client-ip-start client-ip-end*

Parameters

client-ip-start	Specifies an IP address at the start of the range of clients to be allowed access.
client-ip-end	Specifies an IP address at the end of the range of clients to be allowed access.

Defaults

None.

Mode

Router command, SLB Virtual Server Configuration mode: **Matrix>Router(config-slb-vserver)#**

Usage

Specified clients can set up connections directly to the real servers' IP addresses, as well as to the virtual server IP address (VIP). For more information about using this command, see "Configuring Direct Access to Real Servers" on page 19-3.

The "no" form of this command removes non-LSNAT access permission from the specified clients.

Downloaded from www.Manualslib.com manuals search engine

Example

This example shows how to allow clients at 10.24.16.12 through 10.24.16.42 non-LSNAT access to the virtual server named "virtual-http":

```
Matrix>Router(config)#ip slb vserver virtual-http
Matrix>Router(config-slb-vserver)#allow accessservers 10.24.16.12 10.24.16.42
```

ip slb allowaccess_all

Use this command to allow all clients to directly access all services provided by real servers, except for those services configured for server load balancing.

Syntax

ip slb allowaccess_all

no ip slb allowaccess_all

Parameters

None

Defaults

None.

Mode

Router command, Global configuration mode: **Matrix>Router(config)#**

Usage

The real servers are still protected from direct client access for configured services *only*. See "Configuring Direct Access to Real Servers" on page 19-3 for more information about using this command in conjunction with the virtual server configuration mode command **allow accessservers**.

The "no" form of this command removes direct access for all clients.

Examples

This example shows how to allow all clients to have direct access to real servers for all services except those configured for server load balancing:

```
Matrix>Router(config)#ip slb allowaccess_all
```

This example shows how to configure both methods of direct access to real servers. The clients identified with the **allow accessservers** command will have direct access to the real servers for **all** services (including those configured for load-balancing) and be blocked from using the virtual server. All other clients will have direct access to real servers for all services except those configured for server load balancing.

```
Matrix>Router(config)#ip slb allowaccess_all
Matrix>Router(config)#ip slb serverfarm httpserver
Matrix>Router(config-slb-sfarm)#real 10.1.2.1 port 80
Matrix>Router(config-slb-real)#inservice
Matrix>Router(config-slb-real)#exit
Matrix>Router(config-slb-sfarm)#real 10.1.2.3 port 80
```


Downloaded from www.Manualslib.com manuals search engine

```
Matrix>Router(config-slb-real)#inservice
Matrix>Router(config-slb-real)#exit
Matrix>Router(config-slb-sfarm)#exit
Matrix>Router(config)#ip slb vserver virtual-http
Matrix>Router(config-slb-vserver)#serverfarm httpserver
Matrix>Router(config-slb-vserver)#virtual 10.1.4.5 tcp www
Matrix>Router(config-slb-vserver)#persistence level tcp 360
Matrix>Router(config-slb-vserver)#allow accessservers 10.24.16.12 10.24.16.42
Matrix>Router(config-slb-vserver)#inservice
```

show ip slb conns

Use this command to display active server load balancing connections.

Syntax

show ip slb conns [**detail** | **vserver** *virtualserver* [**detail**] | **client** *client-ip* [**detail**]]

Parameters

detail	(Optional) Displays detailed output for a specific virtual server, a specific client, or for all configured virtual servers and clients.
vserver *virtualserver*	(Optional) Specifies a virtual server name for which to display information.
client *client-ip*	(Optional) Specifies a client IP for which to display information.

Defaults

If no parameters are specified, summary information about all active connections will be displayed.

If **detail** is not specified, summary information will be displayed.

Mode

Router command, Any router mode.

Examples

This example shows how to display summary information about active server load balancing connections:

```
Matrix>Router#show ip slb conns

flo-id real-server-ip  client-ip       rport  cl-prt ptcl state
-------------------------------------------------------------------
7      192.169.1.10    192.168.1.137   23     1063   TCP  OUT-SERVR REPLY
6      192.169.2.13    192.168.1.137   1128    *     TCP  OUT-SERVR REPLY
5      192.169.2.13    192.168.1.137   21      *     TCP  OUT-SERVR REPLY
3      192.169.2.14    192.168.1.253   1084    *     TCP  OUT-SERVR REPLY
2      192.169.2.14    192.168.1.253   21      *     TCP  OUT-SERVR REPLY
```


Downloaded from www.Manualslib.com manuals search engine

```
1      192.169.1.11    192.168.1.253   23     1249   TCP  OUT-SERVR REPLY
```

This example shows how to display detailed information about active server load balancing connections:

```
Matrix>Router#show ip slb conns detail
Connection Flow ID : 3
Real Server IP : 172.17.1.2
Client IP : 169.225.1.50
Real Server Port : 1003
Client Port : 1113
Protocol : TCP
Created Time stamp : 2004/3/24 14:34:17
Connection State : outgoing server reply state

Connection Flow ID : 2
Real Server IP : 172.17.1.2
Client IP : 169.225.1.50
Real Server Port : 21
Client Port : 1110
Protocol : TCP
Created Time stamp : 2004/3/24 14:34:07
Connection State : outgoing server reply state
```

Table 19-4 provides an explanation of the detailed command output.

Table 19-4 show ip slb conns Output Details

Output...	What it displays...
Connection Flow ID	Connection flow identifier.
Real Server IP	Address of the real server. Assigned using the **real** command as described in “real” on page 19-8.
Client IP	Client IP address for this connection.
Real Server Port	Real server’s UDP or TCP port assignment.
Client Port	Client’s UDP or TCP port number assignment.
Protocol	Connection protocol: TCP or UDP.
Created Time stamp	Time and date this connection was created.
Connection State	State of the connection.

show ip slb stats

Use this command to display load server balancing statistics.

Syntax

show ip slb stats

Downloaded from www.Manualslib.com manuals search engine

Parameters

None.

Defaults

None.

Mode

Router command, Any router mode.

Example

This example shows how to display server load balancing connection statistics:

```
Matrix>Router#show ip slb stats
created conns      established conns      deleted conns
-------------------------------------------------------------
        3                  2                    1
```

show ip slb sticky

Use this command to display server load balancing active sticky connections.

Syntax

show ip slb sticky [**client** *ip-address*]

Parameters

client *ip-address*	(Optional) Display sticky connections for a particular client.

Defaults

If **client** is not specified, all server load balancing active sticky connections are displayed.

Mode

Router command, Any router mode.

Examples

This example shows how to display all server load balancing active sticky connections.

```
Matrix>Router#show ip slb sticky
client-ip       real-server-ip             conns            ftp-cntrl
-------------------------------------------------------------------------
192.170.1.253   192.169.1.11                 *                2
192.168.1.90    192.169.2.14                 *                0
```


Downloaded from www.Manualslib.com manuals search engine

clear ip slb

Use this command to clear server load balancing counters or to remove server load balancing connections.

Syntax

clear ip slb {[**counters**] [**connections** {**all** | **flowid** *flowid* | **serverfarm** *serverfarm* | **vserver** *vserver*}]}

Parameters

counters	Clears all server load balancing counters.
connections all | **flowid** *flowid* | **serverfarm** *serverfarm* | **vserver** *vserver*	Removes all server load balancing connections, or those associated with a specific flow-ID, server farm name, or virtual server name.

Defaults

If no parameters are specified, all server load balancing counters are cleared and server load balancing connections are removed.

Mode

Router command, Privileged EXEC: **Matrix>Router#**

Example

This example shows how to remove all server load balancing connections:

```
Matrix>Router#clear ip slb connections all
```

show router limits (LSNAT)

Use this command to display LSNAT router limits.

Syntax

show router limits [**lsnat-bindings**] | [**lsnat-cache**] | [**lsnat-configs**]

Parameters

lsnat-bindings	(Optional) Displays the LSNAT maximum bindings limit.
lsnat-cache	(Optional) Displays the LSNAT cache size limit.
lsnat-configs	(Optional) Displays the LSNAT configuration limit.

Defaults

If no options are specified, all router limits will be displayed.

Mode

Switch command, Read-Only.

Downloaded from www.Manualslib.com manuals search engine

Usage

This command must be executed from the switch CLI.

Examples

This example displays all router limits for this system:

```
Matrix(su)->show router limits
LSNAT maximum Bindings                          -  32000  (default)
LSNAT Cache size                                -   2000  (default)
LSNAT maximum Configs                           -     50  (default)
NAT maximum Bindings                            -  32000  (default)
NAT Cache size                                  -   2000  (default)
NAT maximum dynamic mapping Configs             -     10  (default)
NAT maximum static mapping Configs              -     50  (default)
NAT maximum Interface Configs                   -    103  (default)
NAT maximum global address Configs              -   1000  (default)
NAT maximum global port Configs                 -  32000  (default)
Route Table Limit                               -  12000  (default)
TWCB maximum Bindings                           -  32000  (default)
TWCB Cache size                                 -   2000  (default)
TWCB maximum Configs                            -      1  (default)
```

This example displays the LSNAT cache-size limit for this system:

```
Matrix(su)->show router limits lsnat-cache
LSNAT Cache size                                -   2000  (default)
```

set router limits (LSNAT)

Use this command to set LSNAT router limits.

Syntax

set router limits [**lsnat-bindings** *lsnat-bindings*] | [**lsnat-cache** *lsnat-cache*] | [**lsnat-configs** *lsnat-configs*]

Parameters

lsnat-bindings *lsnat-bindings*	(Optional) Sets the LSNAT maximum bindings limit.
lsnat-cache *lsnat-cache*	(Optional) Sets the LSNAT cache size limit.
lsnat-configs *lsnat-configs*	(Optional) Sets the LSNAT configuration limit for the number of server farms, virtual servers, direct access entries, real servers, and client access entries. The *lsnat-configs* value can range from 1 to 50. The number specified will have the following effect: • 1 to 50 server farms, virtual servers, and direct access entries can be configured • 10 to 500 real servers and client access entries can be configured

Downloaded from www.Manualslib.com manuals search engine

Defaults

- If not specified, maximum *bindings* will be set to the default value of 5000.
- If not specified, *cache* size will be set to the default value of 1000.
- If not specified, maximum *configs* will be set to the default value of 50. That is, up to 50 server farms, 50 virtual servers, and 50 direct access entries can be configured, and up to 500 real servers and 500 client access entries can be configured.

Mode

Switch command, Read-Write.

Usage

The chassis or system must be rebooted for any new change to take effect.

This command must be executed from the switch CLI.



Note: Router limits can also be set in the following contexts:

To set NAT router limits see "set router limits (NAT)" on page 18-14.

To set TWCB router limits see "set router limits (TWCB)" on page 23-15.

Example

This example shows how to set the LSNAT configuration limit to 25. This means that up to 25 server farms, 25 virtual servers, and 25 direct access entries can be configured, and up to 250 real servers and 250 client access entries can be configured.

```
Matrix(rw)->set router limits lsnat-configs 25
```

clear router limits (LSNAT)

Use this command to reset chassis-based LSNAT limits to default values.

Syntax

clear router limits [**lsnat-bindings**] | [**lsnat-cache**] | [**lsnat-configs**]

Parameters

lsnat-bindings	(Optional) Resets the LSNAT maximum bindings limit to the default value of 5000.
lsnat-cache	(Optional) Resets the LSNAT cache size limit to the default value of 2000.
lsnat-configs	(Optional) Resets the LSNAT configuration limit to the default value of 50.

Defaults

If no options are specified, all LSNAT limits will be reset.

Downloaded from www.Manualslib.com manuals search engine

Mode

Switch command, Read-Write.

Usage

This command must be executed from the switch CLI.



Note: Router limits can also be cleared in the following contexts:
To clear NAT router limits see “clear router limits (NAT)” on page 18-16.
To clear TWCB router limits see “clear router limits (TWCB)” on page 23-17.

Example

This example shows how to reset all chassis-based LSNAT limits:

```
Matrix(rw)->clear router limits
```


Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

20

DHCP Configuration

This chapter describes the Dynamic Host Configuration Protocol (DHCP) configuration set of commands and how to use them.



Router: Unless otherwise noted, the commands covered in this chapter can be executed only when the device is in router mode. For details on how to enable router configuration modes, refer to "Enabling Router Configuration Modes" on page 2-103.

DHCP Overview

The Dynamic Host Configuration Protocol (DHCP) provides services for allocating and delivering IP addresses and other configuration parameters to Internet hosts. DHCP consists of two components: a protocol for delivering host-specific configuration parameters from a DHCP server to a host, and a mechanism for allocating network addresses to hosts. Optional functionality also provides services to complete high-availability, authenticated and QoS-dependant host configuration.

The DHCP protocol is based on a client-server model in which a designated DHCP server allocates network addresses and delivers configuration parameters to dynamically configured clients. Throughout the remainder of this section, the term "server" refers to a host providing initialization parameters through DHCP, and the term "client" refers to a host requesting initialization parameters from a DHCP server.

DHCP supports the following mechanisms for IP address allocation:

- Automatic — DHCP assigns an IP address to a client for a limited period of time (or until the client explicitly relinquishes the address).
- Manual — A client's IP address is assigned by the network administrator, and DHCP is used simply to convey the assigned address to the client.

The amount of time that a particular IP address is valid for a system is called a lease. The Enterasys Matrix-N or standalone device maintains a lease database which contains information about each assigned IP address, the MAC address to which it is assigned, the lease expiration, and whether the address assignment is dynamic or static. The DHCP lease database is stored in flash memory.

Configuring DHCP

By default, the DHCP server is not enabled on the Enterasys Matrix-N or standalone device. You can selectively enable DHCP service on particular interfaces and not others. To enable DHCP service on an interface, you must first define a DHCP scope. A scope consists of a pool of IP addresses and a set of parameters for a DHCP client. The parameters are used by the client to configure its network environment, for example, the default gateway and DNS domain name.

Downloaded from www.Manualslib.com manuals search engine

To configure DHCP on the Enterasys Matrix-N or standalone device, you must configure an IP address pool, client parameters, and optional static IP address for a specified scope. Where several subnets are accessed through a single port, you can also define multiple scopes on the same interface and group the scopes together into a superscope.

DHCP Task List

The CLI commands for DHCP Server provide functionality for:

1. Configuring a DHCP local pool for a subnet (required)
2. Excluding IP addresses not to be assigned to the clients by the DHCP server (optional)
3. Configuring a DHCP pool (required)
4. Configuring manual bindings of IP addresses and client hardware addresses (optional)
5. Configuring a DHCP server boot file (optional)
6. Monitoring and maintaining DHCP server services (optional)
7. Enabling DHCP service on a routing interface (required)

DHCP Supported Options

Table 20-1 lists the DHCP server option names and codes supported by the firmware. All options specified in Table 20-1 may be configured using the command "option" on page 20-14. Several commonly-used options may also be configured using dedicated commands: "domain-name" on page 20-9, "dns-server" on page 20-10, "netbios-name-server" on page 20-11, "netbios-node-type" on page 20-11, and "default-router" on page 20-12.

Except where noted, all options are defined in RFC-2132. In addition, the site-specific option codes designated by RFC-2132 (128-254) may be used to define options for use within a site or an organization. Some vendors have made use of site-specific options to configure their product features.

Table 20-1 DHCP Server Supported Options

DHCP Option	Option Code
Subnet Mask	**1**
Time Offset	**2**
Router	**3**
Time Server	**4**
Name Server	**5**
Domain Name Server	**6**
Log Server	**7**
Cookie Server	**8**
LPR Server	**9**
Impress Server	**10**
Resource Location Server	**11**
Host Name	**12**
Bootfile Size	**13**
Merit Dump File	**14**

Downloaded from www.Manualslib.com manuals search engine

Table 20-1 DHCP Server Supported Options

DHCP Option	Option Code
Domain Name	**15**
Swap Server	**16**
Root Path	**17**
Extensions Path	**18**
IP Forwarding Enable/Disable	**19**
Non Local Source Routing Enable/Disable	**20**
Policy Filter	**21**
Max Datagram Reassembly Size	**22**
Default IP Time-to-live	**23**
Path MTU Aging Timeout	**24**
Path MTU Plateau Table	**25**
Interface MTU	**26**
All Subnets Are Local	**27**
Broadcast Address	**28**
Perform Mask Discovery	**29**
Mask Supplier	**30**
Perform Router Discovery	**31**
Router Solicitation Address	**32**
Static Route	**33**
Trailer Encapsulation	**34**
ARP Cache Timeout	**35**
Ethernet Encapsulation	**36**
TCP Default TTL	**37**
TCP Keepalive Interval	**38**
TCP Keepalive Garbage	**39**
NIS Domain	**40**
Network Information Servers	**41**
NTP Servers	**42**
Vendor Specific Information	**43**
NetBIOS Over TCP/IP Name Server	**44**
NetBIOS Over TCP/IP Datagram Distribution Server	**45**
NetBIOS Over TCP/IP Node Type	**46**
NetBIOS Over TCP/IP Scope	**47**
X Window System Font Server	**48**
X Window System Display Manager	**49**

Downloaded from www.Manualslib.com manuals search engine

Table 20-1 DHCP Server Supported Options

DHCP Option	Option Code
Renewal Time Value	**58**
Rebinding Time Value	**59**
NIS+ Domain	**64**
NIS+ Servers	**65**
Mobile IP Home Agent	**68**
SMTP Server	**69**
POP3 Server	**70**
NNTP Server	**71**
Default WWW Server	**72**
Default Finger Server	**73**
Default IRC Server	**74**
StreetTalk Server	**75**
StreetTalk Directory Assistance Server	**76**
Relay Agent Information	**82** Defined in RFC-3046
Subnet Selection	**118** Defined in RFC3011

DHCP Command Modes

Except for clear and show commands, most DHCP configuration commands can be executed in most of the DHCP command modes shown in Table 20-2. CLI examples in this section will show a command being executed in one of the appropriate DHCP configuration modes.

Table 20-2 DHCP Command Modes

Mode	Usage	Access Method	Resulting Prompt
IP Local Pool Configuration Mode	Configure a local address pool as a DHCP subnet.	Type **ip local pool** and the local pool *name* from Global Configuration Mode.	**Matrix>Router (ip-local-pool)#**
DHCP Pool Configuration Mode	Configure a DHCP server address pool.	Type **ip dhcp pool** and the address pool *name* from Global Configuration Mode.	**Matrix>Router (config-dhcp-pool)#**

Downloaded from www.Manualslib.com manuals search engine

Table 20-2 DHCP Command Modes (continued)

Mode	Usage	Access Method	Resulting Prompt
DHCP Class Configuration Mode	Configure a DHCP client class.	Type **client-class** and the client class *name* from DHCP Pool or Host Configuration Mode.	**Matrix>Router (config-dhcp-class)#**
DHCP Host Configuration Mode	Configure DHCP host parameters.	Type **client-identifier** and the *identifier*, or **hardware-address** and an *address* from any DHCP configuration mode.	**Matrix>Router (config-dhcp-host)#**

Commands

For information about...	Refer to page...
ip dhcp server	20-6
ip local pool	20-6
exclude	20-7
ip dhcp ping packets	20-8
ip dhcp ping timeout	20-8
ip dhcp pool	20-9
domain-name	20-9
dns-server	20-10
netbios-name-server	20-11
netbios-node-type	20-11
default-router	20-12
bootfile	20-13
next-server	20-13
option	20-14
lease	20-15
host	20-16
client-class	20-16
client-identifier	20-17
client-name	20-18
hardware-address	20-18
show ip dhcp binding	20-19

Downloaded from www.Manualslib.com manuals search engine

For information about...	Refer to page...
clear ip dhcp binding	20-20
show ip dhcp server statistics	20-20
clear ip dhcp server statistics	20-22

ip dhcp server

Use this command to enable DHCP server features on a routing interface.

Syntax

ip dhcp server

no ip dhcp

Parameters

None.

Defaults

None.

Mode

Router command, Interface configuration: **Matrix>Router(config-if(Vlan 1))#**

Usage

The "no" form of this command disables DHCP server features on one or all routing interfaces.

Example

This example shows how to enable DHCP server on VLAN 1:

```
Matrix>Router(config)#interface vlan 1
Matrix>Router(config-if(Vlan 1))ip dhcp server
```

ip local pool

Use this command to configure a local address pool to use as a DHCP subnet. This defines the range of IP addresses to be used by DHCP server and enables IP local pool configuration mode.

Syntax

ip local pool *name subnet mask*

no ip local pool *name subnet mask*

Parameters

name	Specifies a name for the local address pool.
subnet	Specifies an IP subnet for the local address pool.
mask	Specifies a subnet mask for the local address pool. Valid entries are: x.x.x.x or /x.

Downloaded from www.Manualslib.com manuals search engine

Defaults

None.

Mode

Router command, Global configuration: **Matrix>Router(config)#**

Usage

The "no" form of this command removes the local address pool.

Example

This example shows how to configure a local address pool called "localpool" on IP subnet 172.20.28.0/24. Mask can also be expressed as 255.255.255.0:

```
Matrix>Router(config)#ip local pool localpool 172.20.28.0/24
Matrix>Router(ip-local-pool)#
```

exclude

Use this command to exclude one or more addresses from a DHCP local address pool.

Syntax

exclude *ip-address number*

no exclude *ip-address number*

Parameters

ip-address	Specifies the starting IP address to be excluded from this pool.
number	Specifies the number of addresses to be excluded. Valid values are **1** - **65535**.

Defaults

None.

Mode

Router command, IP Local Pool configuration: **Matrix>Router(ip-local-pool)#**

Usage

The "no" form of this command removes the addresses from the list of addresses excluded from the local pool.

Example

This example shows how to exclude 2 IP addresses beginning with 172.20.28.254 from the "localpool" address pool:

```
Matrix>Router(config)#ip local pool localpool
Matrix>Router(ip-local-pool)#exclude 172.20.28.254 2
```


Downloaded from www.Manualslib.com manuals search engine

ip dhcp ping packets

Use this command to specify the number of packets a DHCP server sends to an IP address before assigning the address to a requesting client.

Syntax

ip dhcp ping packets *number*

no ip dhcp ping packets

Parameters

number	Specifies the number of ping packets to be sent. Valid values are **0** - **10**. Default is **2**.

Defaults

None.

Mode

Router command, Global configuration: **Matrix>Router(config)#**

Usage

The "no" form of this command prevents the sever from pinging IP addresses.

Example

This example shows how to set the number of DHCP ping attempts to 6:

```
Matrix>Router(config)#ip dhcp ping packets 6
```

ip dhcp ping timeout

Use this command to specify the amount of time the DHCP server will wait for a ping reply from an IP address before timing out.

Syntax

ip dhcp ping timeout *milliseconds*

no ip dhcp ping timeout

Parameters

milliseconds	Specifies the ping timeout in milliseconds. Valid values are **100** to **10000**. Default: **500** milliseconds.

Defaults

None.

Mode

Router command, Global configuration: **Matrix>Router(config)#**

Downloaded from www.Manualslib.com manuals search engine

Usage

The “no” form of this command resets the ping timeout to the default value.

Example

This example shows how to set the DHCP ping timeout to 900 milliseconds:

```
Matrix>Router(config)#ip dhcp ping timeout 900
```

ip dhcp pool

Use this command to assign a name to a DHCP server pool of addresses, and to enable DHCP address pool configuration mode.

Syntax

ip dhcp pool *name*

no ip dhcp pool *name*

Parameters

name	Specifies a DHCP address pool name. **Note:** This must match the previously configured name assigned with the ip local pool command as described in “ip local pool” on page 20-6.

Defaults

None.

Mode

Router command, Global configuration: **Matrix>Router(config)#**

Usage

The “no” form of this command deletes a DHCP address pool.

Example

This example shows how to assign the name “localpool” as a DHCP address pool, and enable configuration mode for that address pool:

```
Matrix>Router(config)#ip dhcp pool localpool
Matrix>Router(config-dhcp-pool)#
```

domain-name

Use this command to assign a domain name to a DHCP client.

Syntax

domain-name *domain*

no ip dhcp domain-name *domain*

Downloaded from www.Manualslib.com manuals search engine

Parameters

domain	Specifies a domain name string.

Defaults

None.

Mode

Router command, Any DHCP configuration mode.

Usage

This command configures DHCP option 15.

The “no” form of this command deletes a DHCP domain name.

Example

This example shows how to assign the “mycompany.com” domain name to the “localpool” address pool:

```
Matrix>Router(config)#ip dhcp pool localpool
Matrix>Router(config-dhcp-pool)#domain-name mycompany.com
```

dns-server

Use this command to assign one or more DNS servers to DHCP clients.

Syntax

dns-server *address* [*address2...address8*]

no dns-server

Parameters

address	Specifies the IP address of a DNS server.
address2... address8	(Optional) Specifies, in order of preference, up to 7 additional DNS server IP address(es).

Defaults

If *address2...address8* is not specified, no additional addresses will be configured.

Mode

Router command, Any DHCP configuration mode.

Usage

This command configures DHCP option 6.

The “no” form of this command deletes the DNS server list.

Downloaded from www.Manualslib.com manuals search engine

Example

This example shows how to assign a DNS server at 11.12.1.99 to the “localpool” address pool:

```
Matrix>Router(config)#ip dhcp pool localpool
Matrix>Router(config-dhcp-pool)#dns-server 11.12.1.99
```

netbios-name-server

Use this command to assign one or more NetBIOS WINS servers to DHCP clients.

Syntax

netbios-name-server *address* [*address2...address8*]

no netbios-name-server

Parameters

address	Specifies the IP address of a NetBIOS WINS server.
address2... address8	(Optional) Specifies, in order of preference, up to 7 additional NetBIOS WINS server IP address(es).

Defaults

If *address2...address8* is not specified, no additional addresses will be configured.

Mode

Router command, Any DHCP configuration mode.

Usage

This command configures DHCP option 44.

The “no” form of this command deletes the NetBIOS WINS server list.

Example

This example shows how to assign a NetBIOS WINS server at 13.12.1.90 to the “localpool” address pool:

```
Matrix>Router(config)#ip dhcp pool localpool
Matrix>Router(config-dhcp-pool)#netbios-name-server 13.12.1.90
```

netbios-node-type

Use this command to assign a NetBIOS node (server) type to DHCP clients.

Syntax

netbios-node-type *type*

no netbios-node-type

Downloaded from www.Manualslib.com manuals search engine

Parameters

type	Specifies the NetBIOS node type. Valid values and their corresponding types are: • **h-node** — hybrid (recommended) • **b-node** — broadcast • **p-node** — peer-to-peer • **m-mode** — mixed

Defaults

None.

Mode

Router command, Any DHCP configuration mode.

Usage

This command configures DHCP option 46.

The "no" form of this command deletes the NetBIOS node type.

Example

This example shows how to specify hybrid as the NetBIOS node type for the "localpool" address pool:

```
Matrix>Router(config)#ip dhcp pool localpool
Matrix>Router(config-dhcp-pool)#netbios-node type h-node
```

default-router

Use this command to assign a default router list to DHCP clients.

Syntax

default-router *address* [*address2...address8*]

no default-router

Parameters

address	Specifies the IP address of a default router.
address2... address8	(Optional) Specifies, in order of preference, up to 7 additional default router IP address(es).

Defaults

If *address2...address8* is not specified, no additional addresses will be configured.

Mode

Router command, Any DHCP configuration mode.

Downloaded from www.Manualslib.com manuals search engine

Usage

This command configures DHCP option 3.

The "no" form of this command deletes the default router list.

Example

This example shows how to assign a default router at 14.12.1.99 to the “localpool” address pool:

```
Matrix>Router(config)#ip dhcp pool localpool
Matrix>Router(config-dhcp-pool)#default-router 14.12.1.99
```

bootfile

Use this command to specify the default boot image for a DHCP client.

Syntax

bootfile *filename*

no bootfile

Parameters

filename	Specifies the boot image file name.

Defaults

None.

Mode

Router command, Any DHCP configuration mode.

Usage

The “no” form of this command deletes the boot image association.

Example

This example shows how to specify “dhcpboot” as the boot image file in the “localpool” address pool:

```
Matrix>Router(config)#ip dhcp pool localpool
Matrix>Router(config-dhcp-pool)#bootfile dhcpboot
```

next-server

Use this command to specify the next server in the DHCP server boot process.

Syntax

next-server *ip-address*

no next-server *ip-address*

Downloaded from www.Manualslib.com manuals search engine

Parameters

ip-address	Specifies the next server in the boot process by IP address.

Defaults

None.

Mode

Router command, Any DHCP configuration mode.

Usage

The next server is the server the client will contact for the boot file if the primary server is not able to supply it. A next server is usually specified in a manual DHCP binding configuration in order to provide an IP address to a BOOTP client and allow the client to receive the TFTP server address when downloading a boot file image.

The "no" form of this command removes the next server.

Example

This example shows how to specify 192.168.42.13 as the next server in the boot process:

```
Matrix>Router(config)#ip dhcp pool localpool
Matrix>Router(config-dhcp-pool)#next-server 192.168.42.13
```

option

Use this command to configure DHCP options.

Syntax

option *code* [**instance** *number*] {**ascii** *string* | **hex** *string* | **ip** *address*}

no option *code* [**instance** *number*]

Parameters

code	Specifies a DHCP option code. Supported options are specified in Table 20-1 on page 20-2.
instance *number*	(Optional) Assigns an instance number to this option. Valid values are **0** to **255**.
ascii *string* | **hex** *string* | **ip** *address*	Specifies a *code* parameter. An ASCII character string containing a space must be enclosed in quotations.

Defaults

If **instance** is not specified, none (0) will be applied.

Mode

Router command, Any DHCP configuration mode.

Downloaded from www.Manualslib.com manuals search engine

Usage

These configuration parameters and other control information are carried in tagged data items that are stored in the options field of the DHCP message to network hosts. All options specified in Table 20-1 on page 20-2 may be configured using this command. Several commonly-used options may also be configured using dedicated commands: "domain-name" on page 20-9, "dns-server" on page 20-10, "netbios-name-server" on page 20-11, "netbios-node-type" on page 20-11, and "default-router" on page 20-12.

The parameter format of a site-specific option must be either ascii or hex.

The "no" form of this command deletes one or all DHCP options.

Examples

This example shows how to configure DHCP option 19, which specifies whether the client should configure its IP layer for packet forwarding. In this case, IP forwarding is enabled with the 01 value:

```
Matrix>Router(config)#ip dhcp pool localpool
Matrix>Router(config-dhcp-pool)#option 19 hex 01
```

This example shows how to configure DHCP option 72, which assigns one or more Web servers for DHCP clients. In this case, two Web server addresses are configured:

```
Matrix>Router(config)#ip dhcp pool localpool
Matrix>Router(config-dhcp-pool)#option 72 ip 168.24.3.252 168.24.3.253
```

lease

Use this command to specify the duration of the lease for an IP address assigned by a DHCP server to a client.

Syntax

lease {*days* [*hours*] [*minutes*] | **infinite**}

no lease

Parameters

days	Specifies the number of days an address lease will remain valid.
hours	(Optional) When a *days* value has been assigned, specifies the number of hour an address lease will remain valid.
minutes	(Optional) When a *days* value has been assigned, specifies the number of minutes an address lease will remain valid.
infinite	Specifies that the duration of the lease will be unlimited.

Defaults

If *hours* or *minutes* are not specified, no values will be configured.

Mode

Router command, DHCP-Pool, Client-Class and Hardware-Address command modes.

Downloaded from www.Manualslib.com manuals search engine

Usage

The “no” form of this command resets the lease duration to the default value of 1 day (24 hours).

Example

This example shows how to set a one-hour lease to the “localpool” address pool:

```
Matrix>Router(config)#ip dhcp pool localpool
Matrix>Router(config-dhcp-pool)#lease 0 1
```

host

Use this command to specify an IP address and network mask for manual DHCP binding.

Syntax

host *address* [*mask* | *prefix-length*]

no host

Parameters

address	Specifies the IP address of the DHCP client.
mask | *prefix-length*	(Optional) Specifies a network mask or prefix for the IP address.

Defaults

If not specified, DHCP server will examine its defined IP address pools for a *mask* or *prefix-length*. If no mask is found in the IP address pool database, the Class A, B, or C natural mask will be used.

Mode

Router command, DHCP Pool Configuration mode: **Matrix>Router(config-dhcp-pool)#**

Usage

The “no” form of this command removes the client IP address.

Example

This example shows how to set 15.12.1.99 255.255.248.0 as the IP address and subnet mask of a client in the “localpool” address pool:

```
Matrix>Router(config)#ip dhcp pool localpool
Matrix>Router(config-dhcp-pool)#hardware-address 0001.f401.2710
Matrix>Router(config-dhcp-host)#host 15.12.1.99 255.255.248.0
```

client-class

Use this command to identify an DHCP client class.

Syntax

client-class *name*

no client-class *name*

Downloaded from www.Manualslib.com manuals search engine

Parameters

name	Specifies a name for a DHCP client class.

Defaults

None.

Mode

Router command, Any DHCP configuration mode.

Usage

Using this command to give a set of client class properties a name, allows you to assign properties to all DHCP clients within the class rather than configuring each client separately. This command also enables DHCP class configuration mode.

The "no" form of this command deletes a client class name.

Example

This example shows how to assign "clientclass1" as a client class name in the "localpool" address pool:

```
Matrix>Router(config)#ip dhcp pool localpool
Matrix>Router(config-dhcp-pool)#client-class clientclass1
```

client-identifier

Use this command to enable DHCP host configuration mode and associate a client class with a DHCP client.

Syntax

client-identifier *mac-address* [**client-class** *name*]

no client-identifier *unique-identifier*

Parameters

mac-address	Specifies the client's MAC address.
client-class *name*	(Optional) Specifies the class to which this client will be assigned. Must be configured using the client-class name as described in "client-class" on page 20-16.

Defaults

If **client-class** is not specified, none will be assigned.

Mode

Router command, Any DHCP configuration mode.

Usage

The "no" form of this command deletes a client identifier.

Downloaded from www.Manualslib.com manuals search engine

Example

This example shows how to assign client MAC address 00.01f4.0127 within "clientclass1":

```
Matrix>Router(config)#ip dhcp pool localpool
Matrix>Router(config-dhcp-pool)#client-identifier 0100.01f4.0127 client-class
clientclass1
```

client-name

Use this command to assign a name to a DHCP client.

Syntax

client-name *name* [**client-class** *name*]

no client-name *name*

Parameters

name	Specifies a name for a DHCP client. **Note:** The client name should not include the domain name.
client-class *name*	(Optional) Specifies the class to which this client will be assigned. Must be configured using the client-class name as described in "client-class" on page 20-16.

Defaults

If **client-class** is not specified, none will be assigned.

Mode

Router command, Any DHCP configuration mode.

Usage

The "no" form of this command deletes a client name.

Example

This example shows how to assign "soho1" as a client name in "clientclass1":

```
Matrix>Router(config)#ip dhcp pool localpool
Matrix>Router(config-dhcp-pool)#client-name soho1 client-class clientclass1
```

hardware-address

Use this command to specify parameters for a new DHCP client address.

Syntax

hardware-address *hardware-address* [*type*]

no hardware-address *hardware-address* [*type*]

Downloaded from www.Manualslib.com manuals search engine

Parameters

hardware-address	Specifies the MAC address of the client's hardware platform.
type	(Optional) Specifies a hardware protocol or client class name. Valid values and their corresponding meanings are: • **1** - 10Mb Ethernet • **6** or **ieee802** - IEEE 802 networks • **client-class** *name* - Client class (configured as described in "show ip dhcp binding" on page 20-19). • **ethernet** - 10Mb Ethernet

Defaults

If *type* is not specified, Ethernet will be applied.

Mode

Router command, Any DHCP configuration mode.

Usage

This command also enables DHCP host configuration mode.

The "no" form of this command removes the hardware address.

Example

This example shows how to specify 0001.f401.2710 as an Ethernet MAC address for the "localpool" address pool:

```
Matrix>Router(config)#ip dhcp pool localpool
Matrix>Router(config-dhcp-pool)#hardware-address 0001.f401.2710 ethernet
```

show ip dhcp binding

Use this command to display information about one or all DHCP address bindings.

Syntax

show ip dhcp binding [*ip-address*]

Parameters

ip-address	(Optional) Displays bindings for a specific client IP address.

Defaults

If *ip-address* is not specified, information about all address bindings will be shown.

Mode

Router command, Any DHCP configuration mode.

Downloaded from www.Manualslib.com manuals search engine

Example

This example shows how to display the DHCP binding address parameters, including an associated Ethernet MAC addresses, lease expiration dates, type of address assignments, and whether the lease is active:

```
Matrix>(config-dhcp-pool)#show ip dhcp binding

IP address      Hardware address    Lease expiration      Type           Act.
172.28.1.249    00a0.c976.6d38      APR 09 2004 03:33PM   Automatic      Y
172.28.1.254    00a0.ccd1.12f8      Infinite              Manual         Y
```

clear ip dhcp binding

Use this command to delete one or all automatic DHCP address bindings.

Syntax

clear ip dhcp binding {*address* | *****}

Parameters

address | *	Specifies an automatic address binding to be deleted, or that all (*) automatic bindings will be deleted.

Defaults

None.

Mode

Router command, Privileged EXEC: **Matrix>Router#**

Example

This example shows how to delete the address binding 18.12.22.99 from the DHCP server bindings database:

```
Matrix>Router#clear ip dhcp binding 18.12.22.99
```

show ip dhcp server statistics

Use this command to display DHCP server statistics.

Syntax

show ip dhcp server statistics

Parameters

None.

Defaults

None.

Downloaded from www.Manualslib.com manuals search engine

Mode

Router command, Any DHCP configuration mode.

Example

This example shows how to display DHCP server statistics:

```
Matrix>Router#show ip dhcp server statistics

Memory usage           614874
Address pools          3
Database agents        0
Automatic bindings     1
Manual bindings        1
Expired bindings       1
Malformed messages     0

Message                Received
BOOTREQUEST            0
DHCPDISCOVER           0
DHCPREQUEST            646
DHCPDECLINE            0
DHCPRELEASE            0
DHCPINFORM             0

Message                Sent
BOOTREPLY              0
DHCPOFFER              0
DHCPACK                646
DHCPNAK                0
```

Table 20-3 provides an explanation of the command output.

Table 20-3 show ip dhcp server statistics Output Details

Output...	What it displays...
Memory usage	Bytes of RAM allocated by the DHCP server.
Address pools	Configured address pools in the DHCP database.
Database agents	Agents configured in the DHCP database.
Automatic bindings	IP addresses that have been automatically mapped to the Ethernet MAC addresses of hosts found in the DHCP database.
Manual bindings	IP addresses that have been manually mapped to the Ethernet MAC addresses of hosts found in the DHCP database.
Expired bindings	Number of expired leases.
Malformed messages	Number of truncated or corrupted messages e received by the DHCP server.
Message	Message type received by the DHCP server.

Downloaded from www.Manualslib.com manuals search engine

Table 20-3 show ip dhcp server statistics Output Details (continued)

Output...	What it displays...
Received	Number of messages received by the DHCP server.
Sent	Number of messages sent by the DHCP server.

clear ip dhcp server statistics

Use this command to reset all DHCP server counters.

Syntax

```
clear ip dhcp server statistics
```

Parameters

None.

Defaults

None.

Mode

Router command, Privileged EXEC: **Matrix>Router#**

Example

This example shows how to reset all DHCP server counters:

```
Matrix>Router#clear ip dhcp server statistics
```


Downloaded from www.Manualslib.com manuals search engine

21

Routing Protocol Configuration

This chapter describes the Routing Protocol Configuration set of commands and how to use them.



Router: The commands covered in this chapter can be executed only when the device is in router mode. For details on how to enable router configuration modes, refer to "Enabling Router Configuration Modes" on page 2-103.

For information about...	Refer to page...
Activating Advanced Routing Features	21-1
Configuring RIP	21-1
Configuring OSPF	21-19
Configuring DVMRP	21-52
Configuring IRDP	21-55
Configuring VRRP	21-61

Activating Advanced Routing Features

In order to enable advanced routing protocols, such as OSPF and extended ACLs, on an Enterasys Matrix Series device, you must purchase and activate a license key. If you have purchased an advanced routing license, and have enabled routing on the device as described in previous chapters, you can activate your license as described in "Activating Licensed Features" on page 2-58. If you wish to purchase an advanced routing license, contact Enterasys Networks Sales.

Configuring RIP

Purpose

To enable and configure the Routing Information Protocol (RIP).

RIP Configuration Task List and Commands

Table 21-1 lists the tasks and commands associated with RIP configuration. Commands are described in the associated section as shown.



Note: Enabling RIP with the **router rip** and **network** commands is required if you want to run RIP on the device. All other tasks are optional.

Downloaded from www.Manualslib.com manuals search engine

Table 21-1 RIP Configuration Task List and Commands

To do this...	Use these commands...
Enable RIP configuration mode and associate a network.	router rip (“router rip” on page 21-2)
	network (RIP) (“network” on page 21-3)
Allow unicast updates by defining a neighboring router.	neighbor (RIP) (“neighbor” on page 21-4)
Configure an administrative distance.	distance (“distance” on page 21-4)
Apply offsets to RIP routing metrics.	ip rip offset (“ip rip offset” on page 21-5)
Adjust timers.	timers (“timers” on page 21-6)
Specify a RIP version.	ip rip send version (“ip rip send version” on page 21-7)
	ip rip receive version (“ip rip receive version” on page 21-7)
Configure RIP authentication.	Create a key chain (“key chain” on page 21-8)
	Add a key to the chain (“key” on page 21-9)
	Specify an authentication string for the key (“key-string” on page 21-9)
	Set the accept time period the authentication string can be received (“accept-lifetime” on page 21-10)
	Set the send time period the authentication string can be sent as valid (“send-lifetime” on page 21-11)
	Enable a key chain for use on an interface (“ip rip authentication keychain” on page 21-12)
	Specify an authentication mode (“ip rip authentication mode” on page 21-13)
Disable automatic route summarization (necessary for enabling CIDR)	no auto-summary (“no auto-summary” on page 21-13)
Disable triggered updates.	ip rip disable-triggered-updates (“ip rip disable-triggered-updates” on page 21-14)
Disable or re-enable split horizon poison-reverse.	ip split-horizon poison (“ip split-horizon poison” on page 21-15)
Control the processing of routing updates.	passive-interface (“passive-interface” on page 21-15)
	receive interface (“receive-interface” on page 21-16)
	distribute-list (“distribute-list” on page 21-17)
Enable redistribution from non-RIP routes.	redistribute (“redistribute” on page 21-17)

router rip

Use this command to enable or disable RIP configuration mode.

Syntax

```
router rip
no router rip
```


Downloaded from www.Manualslib.com manuals search engine

Parameters

None.

Defaults

None.

Mode

Router command, Global configuration: **Matrix>Router(config)#**

Usage

You must execute the **router rip** command to enable the protocol before completing many RIP-specific configuration tasks. For details on enabling configuration modes, refer to Table 2-8 in "Enabling Router Configuration Modes" on page 2-103.

The "no" form of this command disables RIP.

Example

This example shows how to enable RIP:

```
Matrix>Router#configure terminal
Matrix>Router(config)#router rip
Matrix>Router(config-router)#
```

network

Use this command to attach a network of directly connected networks to a RIP routing process, or to remove a network from a RIP routing process.

Syntax

network *ip-address*

no network *ip-address*

Parameters

ip-address	Specifies the IP address of a directly connected network that RIP will advertise to its neighboring routers.

Defaults

None.

Mode

Router command, Router configuration: **Matrix>Router(config-router)#**

Usage

The "no" form of this command removes the network from the RIP routing process.

Downloaded from www.Manualslib.com manuals search engine

Example

This example shows how to attach network 192.168.1.0 to the RIP routing process:

```
Matrix>Router(config)#router rip
Matrix>Router(config-router)#network 192.168.1.0
```

neighbor

Use this command to instruct the router to send unicast RIP information to an IP address.

Syntax

neighbor *ip-address*

no neighbor *ip-address*

Parameters

ip-address	Specifies the IP address of a directly connected neighbor with which RIP will exchange routing information.

Defaults

None.

Mode

Router command, Router configuration: **Matrix>Router(config-router)#**

Usage

RIP is normally a broadcast protocol. In order for RIP routing updates to reach nonbroadcast networks, the neighbor's IP address must be configured to permit the exchange of routing information.

The "no" form of this command disables point-to-point routing exchanges.

Example

This example shows how to instruct the system to exchange routing information with neighbor 192.5.10.1:

```
Matrix>Router(config)#router rip
Matrix>Router(config-router)#neighbor 192.5.10.1
```

distance

Use this command to configure the administrative distance for RIP routes.

Syntax

distance *weight*

no distance [*weight*]

Downloaded from www.Manualslib.com manuals search engine

Parameters

weight	Specifies an administrative distance for RIP routes. Valid values are **1** - **255**.

Defaults

None.

Mode

Router command, Router configuration: **Matrix>Router(config-router)#**

Usage

If several routes (coming from different protocols) are presented to the Enterasys Matrix Series Route Table Manager (RTM), the protocol with the lowest administrative distance will be chosen for route installation. By default, RIP administrative distance is set to 120. The **distance** command can be used to change this value, resetting RIP's route preference in relation to other routes as shown in the table below.

Route Source	Default Distance
Connected	0
Static	1
OSPF	110
RIP	120

The "no" form of this command resets RIP administrative distance to the default value of 120.

Example

This example shows how to change the default administrative distance for RIP to 1001:

```
Matrix>Router(config)#router rip
Matrix>Router(config-router)#distance 100
```

ip rip offset

Use this command to add or remove an offset to the metric of an incoming or outgoing RIP route.

Syntax

ip rip offset {**in** | **out**} *value*

no ip rip offset {**in** | **out**}

Parameters

in	Applies the offset to incoming metrics.
out	Applies the offset to outgoing metrics.
value	Specifies a positive offset to be applied to routes learned via RIP. Valid values are from **0** to **16**. If the value is 0, no action is taken.

Downloaded from www.Manualslib.com manuals search engine

Defaults

None.

Mode

Router command, Interface configuration: **Matrix>Router(config-if(Vlan 1))#**

Usage

Adding an offset on an interface is used for the purpose of making an interface a backup.

The "no" form of this command removes an offset.

Example

The following example shows how to add an offset of 1 to incoming RIP metrics on VLAN 1:

```
Matrix>Router(config)#interface vlan 1
Matrix>Router(config-if(Vlan 1))#ip rip offset in 1
```

timers

Use this command to adjust RIP routing timers determining the frequency of routing updates, the length of time before a route becomes invalid, and the interval during which routing information regarding better paths is suppressed.

Syntax

timers basic *update-seconds invalid-seconds holdown-seconds flush-seconds*

no timers basic

Parameters

basic	Specifies a basic configuration for RIP routing timers.
update-seconds	Specifies the rate (seconds between updates) at which routing updates are sent. Valid values are **0** to **4294967295**.
invalid-seconds	Specifies the interval (in seconds) after which a route is declared invalid. Valid values are **1** to **4294967295**.
holdown-seconds	Specifies the interval (in seconds) during which routing information regarding better paths is suppressed. Valid values are **0** to **4294967295**.
flush-seconds	Specifies the interval (in seconds) after which a route is deleted. Valid values are **0** to **4294967295**.

Defaults

None.

Mode

Router command, Router configuration: **Matrix>Router(config-router)#**

Usage

The "no" form of this command clears RIP timer parameters.

Downloaded from www.Manualslib.com manuals search engine

Example

This example shows how to set RIP timers to a 5 second update time, a 10 second invalid interval, a 20 second holdown time, and a 60 second flush time:

```
Matrix>Router(config)#router rip
Matrix>Router(config-router)#timers basic 5 10 20 60
```

ip rip send version

Use this command to set the RIP version(s) for update packets transmitted on an interface.

Syntax

ip rip send version {**1** | **2** | **r1compatible**}

no ip rip send version

Parameters

1	Specifies RIP version 1.
2	Specifies RIP version 2.
r1compatible	Specifies that packets be sent as version 2 packets, but transmits these as broadcast packets rather than multicast packets so that systems which only understand RIP version 1 can receive them.

Defaults

None.

Mode

Router command, Interface configuration: **Matrix>Router(config-if(Vlan 1))#**

Usage

The “no” form of this command restores the version of update packets that was transmitted by the RIP module.

Example

This example shows how to set the RIP send version to 2 for packets transmitted on VLAN 1:

```
Matrix>Router(config)#interface vlan 1
Matrix>Router(config-if(Vlan 1))#ip rip send version 2
```

ip rip receive version

Use this command to set the RIP version(s) for update packets accepted on the interface.

Syntax

ip rip receive version {**1** | **2** | **1 2** | **none**}

no ip rip receive version

Downloaded from www.Manualslib.com manuals search engine

Parameters

1	Specifies RIP version 1.
2	Specifies RIP version 2.
1 2	Specifies RIP versions 1 and 2.
none	Specifies that no RIP routes will be processed on this interface.

Defaults

None.

Mode

Router command, Interface configuration: **Matrix>Router(config-if(Vlan 1))#**

Usage

The "no" form of this command restores the default version of the RIP module update packets that are accepted on the interface.

Example

This example shows how to set the RIP receive version to 2 for update packets received on VLAN 1:

```
Matrix>Router(config)#interface vlan 1
Matrix>Router(config-if(Vlan 1))#ip rip receive version 2
```

key chain

Creates or deletes a key chain used globally for RIP authentication.

Syntax

key chain *name*

no key chain *name*

Parameters

name	Specifies a name for the key chain.

Defaults

None.

Mode

Router command, Global configuration: **Matrix>Router(config)#**

Usage

The "no" form of this command deletes the specified key chain.

Downloaded from www.Manualslib.com manuals search engine

Example

This example shows how to create a RIP authentication key chain called “md5key”:

```
Matrix>Router(config)#key chain md5key
```

key

Use this command to identify a RIP authentication key on a key chain.

Syntax

key *key-id*

no key *key-id*

Parameters

key-id	Specifies an authentication number for a key. Valid number are from **0** to **4294967295**. Only one key is supported per key chain in this Enterasys Matrix Series release.

Defaults

None.

Mode

Router command, Key chain configuration: **Matrix>Router(config-keychain)#**

Usage

This release of the Enterasys Matrix Series firmware supports only **one** key per key chain.

The “no” form of this command removes the key from the key chain.

Example

This example shows how to create authentication key 3 within the key chain called “md5key”:

```
Matrix>Router(config-router)#key chain md5key
Matrix>Router(config-keychain)#key 3
```

key-string

Use this command to specify a RIP authentication string for a key. Once configured, this string must be sent and received in RIP packets in order for them to be authenticated.

Syntax

key-string *text*

no key-string *text*

Downloaded from www.Manualslib.com manuals search engine

Parameters

text	Specifies the authentication string that must be sent and received in RIP packets. The string can contain from 1 to 16 uppercase and lowercase alphanumeric characters, except that the first character cannot be a number.

Defaults

None.

Mode

`Router command, Key chain key configuration:` **`Matrix>Router(config-keychain-key)#`**

Usage

The "no" form of this command removes the authentication string.

Example

This example shows how to create an authentication string called "password" for key 3 in the "md5key" key chain:

```
Matrix>Router(config-router)#key chain md5key
Matrix>Router(config-keychain)#key 3
Matrix>Router(config-keychain-key)#key-string password
```

accept-lifetime

Use this command to specify the time period during which an authentication key on a key chain is valid to be received.

Syntax

`accept-lifetime` *`start-time month date year`* {**`duration`** *`seconds`* | *`end-time`* | **`infinite`**}

`no accept-lifetime` *`start-time month date year`*

Parameters

start-time	Specifies the time of day the authentication key will begin to be valid to be received. Valid input is hours:minutes:seconds (*hh:mm:ss*)
month	Specifies the month the authentication key will begin to be valid to be received. Valid input is the first three letters of the month.
date	Specifies the day of the month the authentication key will begin to be valid to be received. Valid values, depending on the length of the month, are **1** - **31**.
year	Specifies the year the authentication key will begin to be valid to be received. Valid input is four digits up to **2035**.
duration *seconds*	Length of time (in seconds) the key is valid to be received. Valid values are **1** - **4294967295**.

Downloaded from www.Manualslib.com manuals search engine

end-time	Specifies the hours, minutes and seconds (*hh:mm:ss)* and the *month*, *date* and *year* from the start-time the key is valid to be received.
infinite	Specifies that the key is valid to be received from the start-time on.

Defaults

None.

Mode

Router command, Key chain key configuration: **Matrix>Router(config-keychain-key)#**

Usage

The "no" form of this command removes the accept-lifetime configuration for an authentication key.

Examples

This example shows how to allow the "password" authentication key to be received as valid on its RIP-configured interface beginning at 2:30 on November 30, 2002 with no ending time (infinitely):

```
Matrix>Router(config-router)#key chain md5key
Matrix>Router(config-keychain)#key 3
Matrix>Router(config-keychain-key)#key-string password
Matrix>Router(config-keychain-key)#accept-lifetime 02:30:00 nov 30 2002 infinite
```

send-lifetime

Use this command to specify the time period during which an authentication key on a key chain is valid to be sent.

Syntax

send-lifetime *start-time month date year* {**duration** *seconds* | *end-time* | **infinite**}

no send-lifetime [*start-time month date year*]

Parameters

start-time	Specifies the time of day the authentication key will begin to be valid to be sent. Valid input is hours:minutes:seconds (*hh:mm:ss*).
month	Specifies the month the authentication key will begin to be valid to be sent. Valid input is the first three letters of the month.
date	Specifies the day of the month the authentication key will begin to be valid to be sent. Valid values, depending on the length of the month, are **1** - **31**.
year	Specifies the year the authentication key will begin to be valid to be sent. Valid input is four digits up to **2035**.
duration *seconds*	Length of time (in seconds) the key is valid to be sent. Valid values are **1** - **4294967295**.
end-time	Specifies the hours, minutes and seconds (*hh:mm:ss)* and the *month*, *date* and *year* from the start-time the key is valid to be sent.
infinite	Specifies that the key is valid to be sent from the start-time on.

Downloaded from www.Manualslib.com manuals search engine

Defaults

None.

Mode

Router command, Key chain key configuration: **Matrix>Router(config-keychain-key)#**

Usage

The "no" form of this command removes the send-lifetime configuration for an authentication key. Start time can be specified, but is not mandatory.

Example

This example shows how to allow the "password" authentication key to be sent as valid on its RIP-configured interface beginning at 2:30 on November 30, 2002 with no ending time (infinitely):

```
Matrix>Router(config-router)#key chain md5key
Matrix>Router(config-keychain)#key 3
Matrix>Router(config-keychain-key)#key-string password
Matrix>Router(config-keychain-key)#send-lifetime 02:30:00 nov 30 2002 infinite
```

ip rip authentication keychain

Use this command to enable or disable a RIP authentication key chain for use on an interface.

Syntax

ip rip authentication keychain *name*

no ip rip authentication keychain *name*

Parameters

name	Specifies the key chain name to enable or disable for RIP authentication.

Defaults

None.

Mode

Router command, Interface configuration: **Matrix>Router(config-if(Vlan 1))#**

Usage

A RIP authentication keychain must be enabled with this command before the RIP authentication mode ("ip rip authentication mode" on page 21-13) can be configured.

The "no" form of this command prevents RIP from using authentication.

Examples

This example shows how to set the RIP authentication key chain to "password" on VLAN 1:

```
Matrix>Router(config)#interface vlan 1
Matrix>Router(config-if(Vlan 1))#ip rip authentication keychain password
```


Downloaded from www.Manualslib.com manuals search engine

ip rip authentication mode

Use this command to set the authentication mode when a key chain is present.

Syntax

```
ip rip authentication mode {text | md5}
no ip rip authentication mode
```

Parameters

text	Initiates text-only authentication.
md5	Initiates MD5 authentication.

Defaults

None.

Mode

Router command, Interface configuration: **Matrix>Router(config-if(Vlan 1))#**

Usage

The RIP authentication keychain must be enabled as described in "ip rip authentication keychain" on page 21-12 before RIP authentication mode can be configured.

The "no" form of this command suppresses the use of authentication.

Example

This example shows how to set the authentication mode for VLAN 1 as "text":

```
Matrix>Router(config)#interface vlan 1
Matrix>Router(config-if(Vlan 1))#ip rip authentication mode text
```

no auto-summary

Use this command to disable automatic route summarization.

Syntax

```
no auto-summary
auto-summary
```

Parameters

None.

Defaults

None.

Mode

Router command, Router configuration: **Matrix>Router(config-router)#**

Downloaded from www.Manualslib.com manuals search engine

Usage

This command is necessary for enabling CIDR for RIP on the Enterasys Matrix Series device.

By default, RIP version 2 supports automatic route summarization, which summarizes subprefixes to the classful network boundary when crossing network boundaries. Disabling automatic route summarization enables CIDR, allowing RIP to advertise all subnets and host routing information on the Enterasys Matrix Series device. To verify which routes are summarized for an interface, use the **show ip protocols** command as described in "show ip protocols" on page 16-22.

The **auto-summary** version of the command re-enables automatic route summarization.

Example

This example shows how to disable RIP automatic route summarization:

```
Matrix>Router(config)#router rip
Matrix>Router(config-router)#no auto-summary
```

ip rip disable-triggered-updates

Use this command to prevent RIP from sending triggered updates.

Syntax

ip rip disable-triggered-updates

no ip rip disable-triggered-updates

Parameters

None.

Defaults

None.

Mode

Router command, Interface configuration: **Matrix>Router(config-if(Vlan 1))#**

Usage

Triggered updates are sent when there is a change in the network and a new route with a lower metric is learned, or an old route is lost. This command stops or starts the interface from sending these triggered updates. By default triggered updates are enabled on a RIP interface.

The "no" form of this command allows RIP to respond to a request for a triggered update.

Example

This example shows how to prevent RIP from responding to a request for triggered updates on VLAN 1:

```
Matrix>Router(config)#interface vlan 1
Matrix>Router(config-if(Vlan 1))#ip rip disable-triggered-updates
```


Downloaded from www.Manualslib.com manuals search engine

ip split-horizon poison

Use this command to enable or disable split horizon poison-reverse mode for RIP packets.

Syntax

ip split-horizon poison

no ip split-horizon poison

Parameters

None.

Defaults

None.

Mode

Router command, Interface configuration: **Matrix>Router(config-if(Vlan 1))#**

Usage

Split horizon prevents packets from exiting through the same interface on which they were received. Poison-reverse explicitly indicates that a network is unreachable, rather than implying it by not including the network in routing updates.

The "no" form of this command disables split horizon poison reverse.

Example

This example shows how to disable split horizon poison reverse for RIP packets transmitted on VLAN 1:

```
Matrix>Router(config)#interface vlan 1
Matrix>Router(config-if(Vlan 1))#no ip split-horizon poison
```

passive-interface

Use this command to prevent RIP from transmitting update packets on an interface.

Syntax

passive-interface vlan *vlan-id*

no passive-interface vlan *vlan-id*

Parameters

vlan *vlan*-id	Specifies the number of the VLAN to make a passive interface. This VLAN must be configured for IP routing as described in "Pre-Routing Configuration Tasks" on page 2-100.

Defaults

None.

Downloaded from www.Manualslib.com manuals search engine

Mode

Router command, Router configuration: **Matrix>Router(config-router)#**

Usage

This command does not prevent RIP from monitoring updates on the interface.

The "no" form of this command disables passive interface.

Example

This example shows how to set VLAN 2 as a passive interface. No RIP updates will be transmitted on VLAN 2:

```
Matrix>Router(config)#router rip
Matrix>Router(config-router)#passive-interface vlan 2
```

receive-interface

Use this command to allow RIP to receive update packets on an interface. This does not affect the sending of RIP updates on the specified interface.

Syntax

receive-interface vlan *vlan-id*

no receive-interface vlan *vlan-id*

Parameters

vlan-id	Specifies the number of the VLAN to make a receive interface. This VLAN must be configured for IP routing as described in "Pre-Routing Configuration Tasks" on page 2-100.

Defaults

None.

Mode

Router command, Router configuration: **Matrix>Router(config-router)#**

Usage

The "no" form of this command denies the reception of RIP updates.

Example

This example shows how to deny the reception of RIP updates on VLAN 2:

```
Matrix>Router(config)#router rip
Matrix>Router(config-router)#no receive-interface vlan 2
```


Downloaded from www.Manualslib.com manuals search engine

distribute-list

Use this command to filter networks received and to suppress networks from being advertised in RIP updates.

Syntax

distribute-list *access-list-number* {**in vlan** *vlan-id* | **out vlan** *vlan-id*}

no distribute-list *access-list-number* {**in vlan** *vlan-id* | **out vlan** *vlan-id*}

Parameters

access-list-number	Specifies the number of the IP access list. This list defines which networks are to be advertised and which are to be suppressed in routing updates. For details on how to configure access lists, refer to "Configuring Access Lists" on page 24-15.
in vlan *vlan-id* | **out vlan** *vlan-id*	Applies the access list to incoming or outgoing routing updates on the specified VLAN. This VLAN must be configured for IP routing as described in "Pre-Routing Configuration Tasks" on page 2-100.

Defaults

None.

Mode

Router command, Router configuration: **Matrix>Router(config-router)#**

Usage

The "no" form of this command removes the filter.

Example

This example shows how to suppress the network 192.5.34.0 from being advertised in outgoing routing updates:

```
Matrix>Router(config)#access-list 1 deny 192.5.34.0 0.0.0.255
Matrix>Router(config)#router rip
Matrix>Router(config-router)#distribute-list 1 out vlan
```

redistribute

Use this command to allow routing information discovered through non-RIP protocols to be distributed in RIP update messages.

Syntax

redistribute {**connected** | **ospf** *process-id* | **static**} [**metric** *metric value*] [**subnets**]

no redistribute {**connected** | **ospf** *process-id* | **static**}

Downloaded from www.Manualslib.com manuals search engine

Parameters

connected	Specifies that non-RIP routing information discovered via directly connected interfaces will be redistributed.
ospf	Specifies that OSPF routing information will be redistributed in RIP.
process-id	Specifies the process ID, an internally used identification number for each instance of the OSPF routing process run on a router. Valid values are **1** to **65535**.
static	Specifies that non-RIP routing information discovered via static routes will be redistributed. Static routes are those created using the **ip route** command detailed in "ip route" on page 16-26.
metric *metric value*	(Optional) Specifies a metric for the connected, OSPF or static redistribution route. This value should be consistent with the designation protocol.
subnets	(Optional) Specifies that connected, OSPF or static routes that are subnetted will be redistributed.

Defaults

- If *metric value* is not specified, 1 will be applied.
- If **subnets** is not specified, only non-subnetted routes will be redistributed.

Mode

Router configuration: **Matrix>Router(config-router)#**

Usage

The "no" form of this command clears redistribution parameters.

Example

This example shows how to redistribute routing information discovered through OSPF process ID 1 non-subnetted routes into RIP update messages:

```
Matrix>Router(config)#router rip
Matrix>Router(config-router)#redistribute ospf 1
```


Downloaded from www.Manualslib.com manuals search engine

Configuring OSPF

Important Notice

OSPF is an advanced routing feature that must be enabled with a license key. If you have purchased an advanced license key, and have enabled routing on the device, you must activate your license as described back in “Activating Licensed Features” on page 2-58 in order to enable the OSPF command set. If you wish to purchase an advanced routing license, contact Enterasys Networks Sales.

Understanding Graceful Restart

OSPF graceful restart, sometimes referred to as non-stop forwarding, provides for an OSPF router to remain on the forwarding path during a restart of its OSPF software. Graceful-restart has four elements to its configuration: enabling, helper router, restart interval, and strict LSA checking.

Enabling graceful restart instructs the firmware to perform a graceful restart, rather than a standard OSPF restart. Restart is only initiated by a fail-over. Grace LSAs are sent when OSPF is restarted on another module. Whether the failover is intentional or not, the failed router protocol is restarted on another module, and upon startup, OSPF sends grace LSAs out to its neighbors using existing link aggregation groups. Use the **graceful-restart enable** command to enable the graceful restart ability on this router.

The helper relationship with the restarting router is on a per network segment basis. The helper monitors the network for topology changes. If no changes occur, the helper router continues to advertise its LSAs as though no restart was occurring. If the restarting router was the designated router, the helper continues to treat it as such. If a topology change does occur, graceful restart is terminated on the restarting router and a standard restart occurs. Helper mode can be disabled on a restarting router neighbor using the **graceful-restart helper-disabled** command. If the restarting router receives an LSA indicating a disabled helper, the graceful restart terminates and a standard restart occurs.

A restart interval provides for a maximum time in seconds after which the graceful restart will terminate should it not complete or terminate for other reasons within the interval. Use the **graceful-restart restart-interval** command to change the restart interval setting.

Strict LSA checking assures that graceful restart will terminate if there is a change to an LSA that would be flooded to the restarting router. Strict LSA checking can be disabled. If disabled, a change to an LSA that would be flooded to the restarting router will not cause the graceful restart to terminate. Use the **graceful-restart strict-lsa-checking-disabled** command to disable strict LSA checking.

View the router OSPF section of the **show running-config** display to verify any non-default graceful restart settings.

Graceful Restart and High Availability

The DFE supports single router high availability failover using the following components:

- OSPF graceful restart
- Non-stop router frame forwarding on each module
- Single router configuration
- Router protocol process failover to another module
- Link Aggregate Group (LAG) connectivity to neighboring routers

The DFE is a distributed routing system. The routing protocol process resides on a single router module. Information such as access list rules, policy routing rules, interface configuration and best routes are calculated by the protocol process and distributed to all modules. Each module has its

Downloaded from www.Manualslib.com manuals search engine

own forwarding engine that uses this information to make forwarding decisions locally on the module that receives the frame. These engines independently make forwarding decisions based on route and rule information distributed by the router protocol process. In a stable network, the distributed route and rule information is fairly constant. If the router protocol process was to suddenly fail, forwarding information current at the time of the failure in all probability is usable for the short time after the failure until recovery occurs. During this recovery period, existing connections (that were not directly using the failed module) remain in effect. New connections continue to be installed using the last known "good" forwarding information. The router protocol process that failed is dynamically restarted on another module. The user does not configure where the router process is running. The router forwarding process remains active on every module. The protocol process exchanges protocol and maintains state that it distributes to the other modules and does not have to run on any specific module. One exception to this rule is that the module must have 256M of memory to be router protocol process eligible.

Upon failure of a module running the router protocol process, the protocol process is started on a recovery module. One of the first messages it sends to its OSPF neighbors is a grace LSA. High availability failover will successfully occur if the following is true:

- The router is enabled for graceful restart
- The neighbors are enabled to participate as graceful restart helper
- The OSPF dead interval is configured for a sufficient period such that the grace LSA is received by its neighbors before the configured OSPF dead interval expires
- And each neighbor is a member of a LAG common to the failed router, allowing the neighbor to remain up

Figure 21-1 Physical and Logical Single Router HA Failover Configuration

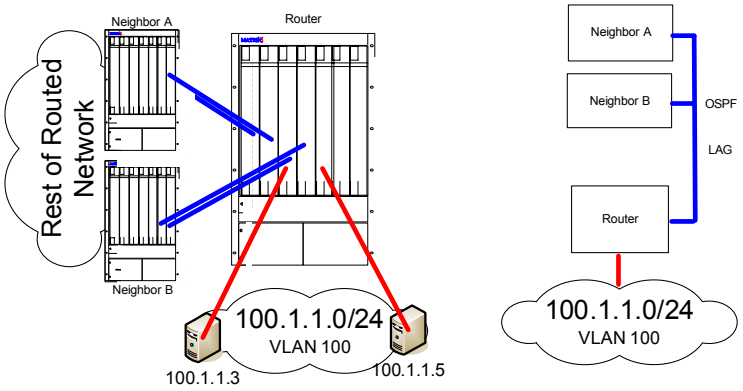


Figure 21-1 depicts the physical and logical configurations of the single router high availability failover mechanism. The blue lines display direct neighbor connections to the router enabled for OSPF graceful restart and members of LAGs common to the failing router. The red lines display VLAN connections common to both the failing and recovery routers.

Purpose

To enable and configure the Open Shortest Path First (OSPF) routing protocol.

Downloaded from www.Manualslib.com manuals search engine

OSPF Configuration Task List and Commands

Table 21-2 lists the tasks and commands associated with OSPF configuration. Commands are described in the associated section as shown.



Note: Activating your advanced routing license, and enabling OSPF with the **router ospf** and **network** commands are required if you want to run OSPF on the device. All other tasks are optional.

Table 21-2 OSPF Configuration Task List and Commands

To do this...	Use these commands...
If necessary, activate your advanced routing license.	set license (“set license” on page 2-58)
Enable OSPF configuration mode, associate a network and assign a router ID.	router ospf (“router ospf” on page 21-22)
	network (“network” on page 21-23)
	router id (“router id” on page 21-24)
Configure OSPF Interface Parameters.	
Set the cost of sending a packet on an OSPF interface.	ip ospf cost (“ip ospf cost” on page 21-24)
Set a priority to help determine the OSPF designated router for the network.	ip ospf priority (“ip ospf priority” on page 21-25)
Adjust timers and message intervals.	timers spf (“timers spf” on page 21-26)
	ip ospf retransmit-interval (“ip ospf retransmit-interval” on page 21-26)
	ip ospf transmit-delay (“ip ospf transmit-delay” on page 21-27)
	ip ospf hello-interval (“ip ospf hello-interval” on page 21-28)
	ip ospf dead-interval (“ip ospf dead-interval” on page 21-28)
Configure OSPF authentication.	ip ospf authentication-key (“ip ospf authentication-key” on page 21-29)
	ip ospf message digest key md5 (“ip ospf message digest key md5” on page 21-30)
Configure OSPF Areas.	
Configure an administrative distance.	distance ospf (“distance ospf” on page 21-30)
Define the range of addresses to be used by Area Boundary Routers (ABRs).	area range (“area range” on page 21-31)
Enable area authentication.	area authentication (“area authentication” on page 21-32)
Define an area as a stub area.	area stub (“area stub” on page 21-33)
Set the cost value for the default route that is sent into a stub area.	area default cost (“area default cost” on page 21-34)
Define an area as an NSSA.	area nssa (“area nssa” on page 21-34)
Create virtual links.	area virtual-link (“area virtual-link” on page 21-35)

Downloaded from www.Manualslib.com manuals search engine

Table 21-2 OSPF Configuration Task List and Commands (continued)

To do this...	Use these commands...
Enable passive OSPF mode on an interface.	passive-interface (“passive-interface” on page 21-36)
Enable redistribution from non-OSPF routes.	redistribute (“redistribute” on page 21-37)
Limit link state database overflow.	database-overflow (“database-overflow” on page 21-38)
Enable graceful restart	graceful-restart enable (“graceful-restart enable” on page 21-39)
Disable graceful restart helper	graceful-restart helper-disable (“graceful-restart helper-disable” on page 21-40)
Setting the graceful restart restart-interval	graceful-restart restart-interval (“graceful-restart restart-interval” on page 21-40)
Disabling strict LSA checking for graceful restart	graceful-restart strict-lsa-checking-disable (“graceful-restart strict-lsa-checking-disable” on page 21-41)
Monitor and maintain OSPF.	show ip ospf (“show ip ospf” on page 21-42)
	show ip ospf database (“show ip ospf database” on page 21-43)
	show ip ospf border-routers (“show ip ospf border-routers” on page 21-45)
	show ip ospf interface (“show ip ospf interface” on page 21-45)
	show ip ospf neighbor (“show ip ospf neighbor” on page 21-47)
	show ip ospf virtual-links (“show ip ospf virtual-links” on page 21-48)
	clear ip ospf process (“clear ip ospf process” on page 21-49)
	debug ip ospf (“debug ip ospf” on page 21-50)
Enable RFC1583 compatibility	rfc1583compatible (“rfc1583compatible” on page 21-50)

router ospf

Use this command to enable or disable Open Shortest Path First (OSPF) configuration mode.

Syntax

router ospf *process-id*

no router ospf *process-id*

Parameters

process-id	Specifies the process ID, an internally used identification number for an OSPF routing process run on a router. Only one OSPF process is allowed per device. Valid values are **1** to **65535**.

Defaults

None.

Downloaded from www.Manualslib.com manuals search engine

Mode

Router command, Global configuration: **Matrix>Router(config)#**

Usage

You must execute the **router ospf** command to enable the protocol before completing many OSPF-specific configuration tasks. For details on enabling configuration modes, refer to Table 2-8 in "Enabling Router Configuration Modes" on page 2-103.

Only one OSPF process (*process-id*) is allowed per Enterasys Matrix Series routing module or standalone device.

The "no" form of this command disables OSPF configuration mode.

Example

This example shows how to enable routing for OSPF process 1:

```
Matrix>Router#conf terminal
Matrix>Router(config)#router ospf 1
Matrix>Router(config-router)#
```

network

Use this command to configure area IDs for OSPF interfaces.

Syntax

network *ip-address wildcard-mask* **area** *area-id*

no network *ip-address wildcard-mask* **area** *area-id*

Parameters

ip-address	Specifies the IP address of an interface or a group of interfaces within the network address range.
wildcard-mask	Specifies the IP-address-type mask that includes "don't care" bits.
area *area-id*	Specifies the *area-id* to be associated with the OSPF address range. Valid values are decimal values or IP addresses. A subnet address can be specified as the *area-id* to associate areas with IP subnets.

Defaults

None.

Mode

Router command, Router configuration: **Matrix>Router(config-router)#**

Usage

The "no" form of this command removes OSPF routing for interfaces identified by the IP address and mask parameters.

Downloaded from www.Manualslib.com manuals search engine

Example

This example shows how to configure IP address 182.127.62.1 0.0.0.31 as OSPF area 0:

```
Matrix>Router(config)#router ospf 1
Matrix>Router(config-router)#network 182.127.62.1 0.0.0.31 area 0
```

router id

Use this command to set the OSPF router ID for the device.

Syntax

router id *ip-address*

no router id

Parameters

ip-address	Specifies the IP address that OSPF will use as the router ID.

Defaults

None.

Mode

Router command, Router configuration: **Matrix>Router(config-router)#**

Usage

The OSPF protocol uses the router ID as a tie-breaker for path selection. If not specified, this will be set to the lowest IP address of the interfaces configured for IP routing.

The "no" form of this command resets the router ID to the first interface configured for IP routing.

Example

This example shows how to set the OSPF router ID to IP address 182.127.62.1:

```
Matrix>Router(config-router)#router id 182.127.62.1
```

ip ospf cost

Use this command to set the cost of sending an OSPF packet on an interface.

Syntax

ip ospf cost *cost*

no ip ospf *cost*

Parameters

cost	Specifies the cost of sending a packet. Valid values range from **1** to **65535**.

Defaults

None.

Downloaded from www.Manualslib.com manuals search engine

Mode

Router command, Interface configuration: **Matrix>Router(config-if(Vlan 1))#**

Usage

Each router interface that participates in OSPF routing is assigned a default cost. This command overwrites the default of 10.

The "no" form of this command resets the OSPF cost to the default of 10.

Example

This example shows how to set the OSPF cost to 20 for VLAN 1:

```
Matrix>Router(config)#interface vlan 1
Matrix>Router(config-if(Vlan 1))#ip ospf cost 20
```

ip ospf priority

Use this command to set the OSPF priority value for router interfaces.

Syntax

ip ospf priority *number*

no ip ospf priority

Parameters

number	Specifies the router's OSPF priority in a range from **0** to **255**.

Defaults

None.

Mode

Router command, Interface configuration: **Matrix>Router(config-if(Vlan 1))#**

Usage

The priority value is communicated between routers by means of hello messages and influences the election of a designated router.

The "no" form of this command resets the value to the default of 1.

Example

This example shows how to set the OSPF priority to 20 for VLAN 1:

```
Matrix>Router(config)#interface vlan 1
Matrix>Router(config-if(Vlan 1))#ip ospf priority 20
```


Downloaded from www.Manualslib.com manuals search engine

timers spf

Use this command to change OSPF timer values to fine-tune the OSPF network.

Syntax

timers spf *spf-delay spf-hold*

no timers spf

Parameters

spf-delay	Specifies the delay, in seconds, between the receipt of an update and the SPF execution. Valid values are **0** to **4294967295**. Default **5** Seconds.
spf-hold	Specifies the minimum amount of time, in seconds, between two consecutive OSPF calculations. A value of 0 means that two consecutive OSPF calculations are performed one immediately after the other. Valid values are **0** to **4294967295**. Default: **10** Seconds.

Defaults

None.

Mode

Router command, Router configuration: **Matrix>Router(config-router)#**

Usage

The "no" form of this command restores the default timer values.

Example

This example shows how to set spf delay time to 7 seconds and hold time to 3:

```
Matrix>Router(config)#ospf 1
Matrix>Router(config-router)#timers spf 7 3
```

ip ospf retransmit-interval

Use this command to set the amount of time between retransmissions of link state advertisements (LSAs) for adjacencies that belong to an interface.

Syntax

ip ospf retransmit-interval *seconds*

no ip ospf retransmit-interval

Parameters

seconds	Specifies the retransmit time in seconds. Valid values are **1** to **65535**. Default: 5 Seconds.

Defaults

None.

Downloaded from www.Manualslib.com manuals search engine

Mode

Router command, Interface configuration: **Matrix>Router(config-if(Vlan 1))#**

Usage

The "no" form of this command resets the retransmit interval value to the default.

Example

This example shows how to set the OSPF retransmit interval for VLAN 1 to 20:

```
Matrix>Router(config)#interface vlan 1
Matrix>Router(config-if(Vlan 1))#ip ospf retransmit-interval 20
```

ip ospf transmit-delay

Use this command to set the amount of time required to transmit a link state update packet on an interface.

Syntax

ip ospf transmit-delay *seconds*

no ip ospf transmit-delay

Parameters

seconds	Specifies the transmit delay in seconds. Valid values are from **1** to **65535**. Default: **1** Second.

Defaults

None.

Mode

Router command, Interface configuration: **Matrix>Router(config-if(Vlan 1))#**

Usage

The "no" form of this command resets the retransmit interval value to the default.

Example

This example shows how to set the time required to transmit a link state update packet on VLAN 1 at 20 seconds:

```
Matrix>Router(config)#interface vlan 1
Matrix>Router(config-if(Vlan 1))#ip ospf transmit-delay 20
```


Downloaded from www.Manualslib.com manuals search engine

ip ospf hello-interval

Use this command to set the number of seconds a router must wait before sending a hello packet to neighbor routers on an interface.

Syntax

ip ospf hello-interval *seconds*

no ip ospf hello-interval

Parameters

seconds	Specifies the hello interval in seconds. Hello interval must be the same on neighboring routers (on a specific subnet), but can vary between subnets. This parameter is an unsigned integer with valid values between **1** and **65535**. Defaults: **10** seconds for broadcast and point-to-point networks; **30** seconds for non-broadcast and point-to-multipoint networks.

Defaults

None.

Mode

Router command, Interface configuration: **Matrix>Router(config-if(Vlan 1))#**

Usage

Each Enterasys Matrix Series routing module or standalone device can support communications between up to 60 neighboring routers.

The "no" form of this command sets the hello interval value to the default.

Example

This example shows how to set the hello interval to 5 for VLAN 1:

```
Matrix>Router(config)#interface vlan 1
Matrix>Router(config-if(Vlan 1))#ip ospf hello-interval 5
```

ip ospf dead-interval

Use this command to set the number of seconds a router must wait to receive a hello packet from its neighbor before determining that the neighbor is out of service.

Syntax

ip ospf dead-interval *seconds*

no ip ospf dead-interval

Parameters

seconds	Specifies the number of seconds that a router must wait to receive a hello packet. Dead interval must be the same on neighboring routers (on a specific subnet), but can vary between subnets. This parameter is an unsigned integer ranging from **1** to **65535**. Default: **40** Seconds.

Downloaded from www.Manualslib.com manuals search engine

Defaults

None.

Mode

Router command, Interface configuration: **Matrix>Router(config-if(Vlan 1))#**

Usage

The "no" form of this command sets the dead interval value to the default.

Example

This example shows how to set the dead interval to 20 for VLAN 1:

```
Matrix>Router(config)#interface vlan 1
Matrix>Router(config-if(Vlan 1))#ip ospf dead-interval 20
```

ip ospf authentication-key

Use this command to assign a password to be used by neighboring routers using OSPF's simple password authentication.

Syntax

ip ospf authentication-key *password*

no ip ospf authentication-key

Parameters

password	Specifies an OSPF authentication password. Valid values are alphanumeric strings up to 8 bytes in length.

Defaults

If *password* is not specified, the password will be set to a blank string.

Mode

Router command, Interface configuration: **Matrix>Router(config-if(Vlan 1))#**

Usage

The password key set with this command will only be used when authentication is enabled for an OSPF area using the **area authentication** command described in "area authentication" on page 21-32.

All neighboring routers on the same network must have the same password configured to be able to exchange OSPF information.

This password is used as a "key" that is inserted directly into the OSPF header in routing protocol packets. A separate password can be assigned to each OSPF network on a per-interface basis.

The "no" form of this command removes an OSPF authentication password on an interface.

Downloaded from www.Manualslib.com manuals search engine

Example

This example shows how to enables an OSPF authentication key on VLAN 1 with the password "yourpass":

```
Matrix>Router(config)#interface vlan 1
Matrix>Router(config-if(Vlan 1))#ip ospf authentication-key yourpass
```

ip ospf message digest key md5

Use this command to enable or disable OSPF MD5 authentication on an interface.

Syntax

ip ospf message-digest-key *keyid* **md5** *key*

no ip ospf message-digest-key *keyid*

Parameters

keyid	Specifies the key identifier on the interface where MD5 authentication is enabled. Valid values are integers from **1** to **255**.
key	Specifies a password for MD5 authentication to be used with the *keyid*. Valid values are alphanumeric strings of up to 16 bytes.

Defaults

None.

Mode

Router command, Interface configuration: **Matrix>Router(config-if(Vlan 1))#**

Usage

This command validates OSPF MD5 routing updates between neighboring routers.

The "no" form of this command disables MD5 authentication on an interface.

Example

This example shows how to enable OSPF MD5 authentication on VLAN 1, set the key identifier to 20, and set the password to "passone":

```
Matrix>Router(config)#interface vlan 1
```

Matrix>Router(config-if(Vlan 1))#ip ospf message-digest-key 20 md5 passone

distance ospf

Use this command to configure the administrative distance for OSPF routes.

Syntax

distance ospf {**external** | **inter-area** | **intra-area**} *weight*

no distance ospf {**external** | **inter-area** | **intra-area**}

Downloaded from www.Manualslib.com manuals search engine

Parameters

external | **inter-area** | **intra-area**	Applies the distance value to external (type 5 and type 7), to inter-area, or to intra-area routes. **Note:** The value for intra-area distance must be less than the value for inter-area distance, which must be less than the value for external distance.
weight	Specifies an administrative distance for OSPF routes. Valid values are **1** - **255**.

Defaults

If route type is not specified, the distance value will be applied to all OSPF routes (110).

Mode

Router command, Router configuration: **Matrix>Router(config-router)#**

Usage

If several routes (coming from different protocols) are presented to the Enterasys Matrix Series Route Table Manager (RTM), the protocol with the lowest administrative distance will be chosen for route installation. By default, OSPF administrative distance is set to 110. The **distance ospf** command can be used to change this value, resetting OSPF's route preference in relation to other routes as shown in the table below.

Route Source	Default Distance
Connected	0
Static	1
OSPF	110
RIP	120

The "no" form of this command resets OSPF administrative distance to the default value of 110.

Example

This example shows how to change the default administrative distance for external OSPF routes to 100:

```
Matrix>Router(config)#router ospf 1
Matrix>Router(config-router)#distance ospf external 100
```

area range

Use this command to define the range of addresses to be used by Area Border Routers (ABRs) when they communicate routes to other areas.

Syntax

area *area-id* **range** *ip-address ip-mask*

no area *area-id* **range** *ip-address ip-mask*

Downloaded from www.Manualslib.com manuals search engine

Parameters

area-id	Specifies the area at the boundary of which routes are to be summarized.
ip-address	Specifies the common prefix of the summarized networks.
ip-mask	Specifies the length of the common prefix.

Defaults

None.

Mode

Router command, Router configuration: **Matrix>Router(config-router)#**

Usage

Each Enterasys Matrix Series module or standalone device can support up to 6 OSPF areas and up to 256 OSPF interfaces running per Enterasys Matrix chassis.

The "no" form of this command stops the routes from being summarized.

Example

This example shows how to define the address range as 172.16.0.0/16 for summarized routes communicated at the boundary of area 0.0.0.0:

```
Matrix>Router(config)#router ospf 1
Matrix>Router(config-router)#area 0.0.0.0 range 172.16.0.0 255.255.0.0
```

area authentication

Use this command to enable or disable authentication for an OSPF area.

Syntax

area *area-id* **authentication** {**simple** | **message-digest**}

no area *area-id* **authentication** {**simple** | **message-digest**}

Parameters

area-id	Specifies the OSPF area in which to enable authentication. Valid values are decimal values or IP addresses.
simple	Enables simple text authentication. Simple password authentication allows a password (key) to be configured per area. Routers in the same area that want to participate in the routing domain will have to be configured with the same key.
message-digest	Enables MD5 authentication on the OSPF area indicated by the *area-id*.

Defaults

None.

Mode

Router command, Router configuration: **Matrix>Router(config-router)#**

Downloaded from www.Manualslib.com manuals search engine

Usage

The “no” form of this command disables authentication for an OSPF area.

Example

This example shows how to enable MD5 authentication on OSPF area 10.0.0.0:

```
Matrix>Router(config)#router ospf 1
Matrix>Router(config-router)#area 10.0.0.0 authentication message-digest
```

area stub

Use this command to define an OSPF area as a stub area.

Syntax

area *area-id* **stub** [**no-summary**]

no area *area-id* **stub** [**no-summary**]

Parameters

area-id	Specifies the stub area. Valid values are decimal values or ip addresses.
no-summary	(Optional) Prevents an Area Border Router (ABR) from sending Link State Advertisements (LSAs) into the stub area. When this parameter is used, it means that all destinations outside of the stub area are represented by means of a default route.

Defaults

If **no-summary** is not specified, the stub area will be able to receive LSAs.

Mode

Router command, Router configuration: **Matrix>Router(config-router)#**

Usage

This is an area that carries no external routes.

The “no” form of this command changes the stub back to a plain area.

Example

The following example shows how to define OSPF area 10 as a stub area:

```
Matrix>Router(config)#router ospf 1
Matrix>Router(config-router)#area 10 stub
```


Downloaded from www.Manualslib.com manuals search engine

area default cost

Use this command to set the cost value for the default route that is sent into a stub area by an Area Border Router (ABR).

Syntax

area *area-id* **default-cost** *cost*

no area *area-id* **default-cost**

Parameters

area-id	Specifies the stub area. Valid values are decimal values or IP addresses.
cost	Specifies a cost value for the summary route that is sent into a stub area by default. Valid values are 24-bit numbers, from **0** to **16777215**.

Defaults

None.

Mode

Router command, Router configuration: **Matrix>Router(config-router)#**

Usage

The use of this command is restricted to ABRs attached to stub areas.

The "no" form of this command removes the cost value from the summary route that is sent into the stub area.

Example

This example shows how to set the cost value for stub area 10 to 99:

```
Matrix>Router(config)#router ospf 1
Matrix>Router(config-router)#area 10 default-cost 99
```

area nssa

Use this command to configure an area as a not so stubby area (NSSA).

Syntax

area *area-id* **nssa** [**default-information-originate**]

no area *area-id* **nssa** [**default-information-originate**]

Parameters

area-id	Specifies the NSSA area. Valid values are decimal values or IP addresses.
default-information-originate	(Optional) Generates a default of Type 7 into the NSSA. This is used when the router is an NSSA ABR.

Downloaded from www.Manualslib.com manuals search engine

Defaults

If **default-information-originate** is not specified, no default type will be generated.

Mode

Router command, Router configuration: **Matrix>Router(config-router)#**

Usage

An NSSA allows some external routes represented by external Link State Advertisements (LSAs) to be imported into it. This is in contrast to a stub area that does not allow any external routes. External routes that are not imported into an NSSA can be represented by means of a default route. This configuration is used when an OSPF internetwork is connected to multiple non-OSPF routing domains.

The "no" form of this command changes the NSSA back to a plain area.

Example

This example shows how to configure area 10 as an NSSA area:

```
Matrix>Router(config)#router ospf 1
Matrix>Router(config-router)#area 10 nssa default-information-originate
```

area virtual-link

Use this command to define an OSPF virtual link, which represents a logical connection between the backbone and a non-backbone OSPF area.

Syntax

area *area-id* **virtual-link** *ip-address*

The options for using this syntax are:

area *area-id* **virtual-link** *ip-address* **authentication-key** *key*
area *area-id* **virtual-link** *ip-address* **dead-interval** *seconds*
area *area-id* **virtual-link** *ip-address* **hello-interval** *seconds*
area *area-id* **virtual-link** *ip-address* **retransmit-interval** *seconds*
area *area-id* **virtual-link** *ip-address* **transmit-delay** *seconds*
no area *area-id* **virtual-link** *ip-address* **authentication-key** *key*
no area *area-id* **virtual-link** *ip-address* **dead-interval** *seconds*
no area *area-id* **virtual-link** *ip-address* **hello-interval** *seconds*
no area *area-id* **virtual-link** *ip-address* **retransmit-interval** *seconds*
no area *area-id* **virtual-link** *ip-address* **transmit-delay** *seconds*

Parameters

area-id	Specifies the transit area for the virtual link. Valid values are decimal values or IP addresses. A transit area is an area through which a virtual link is established.
ip-address	Specifies the IP address of the ABR. A virtual link is established from the ABR, where virtual link configuration is taking place.

Downloaded from www.Manualslib.com manuals search engine

authentication- key *key*	Specifies a password to be used by neighbor routers. Valid values are alphanumeric strings of up to 8 bytes. Neighbor routers on a network must have the same password.
dead-interval *seconds*	Specifies the number of seconds that the hello packets of a router are not communicated to neighbor routers before the neighbor routers determine that the router sending the hello packet is out of service. This value must be the same for all nodes attached to a certain subnet, and it is a value ranging from **1** to **8192**.
hello-interval *seconds*	Specifies the number of seconds between hello packets on an interface. This value must be the same for all nodes attached to a network and it is a value ranging from **1** to **8192**.
retransmit-interval *seconds*	Specifies the number of seconds between successive retransmissions of the same LSAs. Valid values are greater than the expected amount of time required for the update packet to reach and return from the interface, and range from **1** to **8192**.
transmit-delay *seconds*	Specifies the estimated number of seconds for a link state update packet on the interface to be transmitted. Valid values range from **1** to **8192**.

Defaults

None.

Mode

Router command, Router configuration: **Matrix>Router(config-router)#**

Usage

The “no” form of this command removes the virtual link.

Example

This example shows how to configure a virtual link between OSPF area 0.0.0.2 and ABR network 134.141.7.2:

```
Matrix>Router(config)#router ospf 1
Matrix>Router(config-router)#area 0.0.0.2 virtual-link 134.141.7.2
```

passive-interface

Use this command to enable passive OSPF on an interface.

Syntax

passive-interface vlan *vlan-id*

no passive-ospf vlan *vlan-id*

Parameters

vlan-id	Specifies the interface on which to enable passive OSPF mode.

Defaults

None.

Downloaded from www.Manualslib.com manuals search engine

Mode

Router command, Router configuration: **Matrix->Router(config-router)#**

Usage

This allows an interface to be included in the OSPF route table, but turns off sending and receiving hellos for an interface. It also prevents OSPF adjacencies from being formed on an interface.

The "no" form of this command disables passive OSPF mode.

Example

This example shows how to enable passive OSPF mode on VLAN 102:

```
Matrix->Router(config)#router ospf 1
Matrix->Router(config-router)#passive-interface vlan 102
```

redistribute

Use this command to allow routing information discovered through non-OSPF protocols to be distributed in OSPF update messages.

Syntax

redistribute {**rip** | **static** [**metric** *metric value*] [**metric-type** *type-value*] [**subnets**] [**tag**] [**route-map** *id-number*] | {**connected** [**route-map** *id-number*] [**metric** *metric value*] [**metric-type** *type-value*] [**subnets**] [**tag** *tag*]}

no redistribute {**connected** | **rip** | **static**}

Parameters

rip	Specifies that RIP routing information will be redistributed in OSPF.
static	Specifies that non-OSPF information discovered via static routes will be redistributed. Static routes are those created using the **ip route** command detailed in "ip route" on page 16-26.
metric *metric value*	(Optional) Specifies a metric for the connected, RIP or static redistribution route. This value should be consistent with the designation protocol.
metric-type *type value*	(Optional) Specifies the external link type associated with the default connected, RIP or static route advertised into the OSPF routing domain. Valid values are **1** for type 1 external route, and **2** for type 2 external route.
subnets	(Optional) Specifies that connected, RIP or static routes that are subnetted routes will be redistributed.
tag *tag*	(Optional) Specifies that tagged routes will be redistributed in OSPF.
connected	Specifies that non-OSPF information discovered via directly connected interfaces will be redistributed. These are routes not specified in the OSPF network command as described in "network" on page 21-23.
route-map *id-number*	(Optional) Redistributes routes using the rules established by the designated route-map. Valid values are 1-99.

Downloaded from www.Manualslib.com manuals search engine

Defaults

- If *metric value* is not specified, 0 will be applied.
- If *type value* is not specified, type 2 (external route) will be applied.
- If **subnets** is not specified, only non-subnetted routes will be redistributed.
- If **route-map** is not specified, none will be applied.
- If **tag** is not specified, none will be applied.

Mode

Router configuration: **Matrix>Router(config-router)#**

Usage

The "no" form of this command clears redistribution parameters.

Example

This example shows how to distribute external type 2 RIP routing information from non-subnetted routes in OSPF updates:

```
Matrix>Router(config)#router ospf
Matrix>Router(config-router)#redistribute rip
```

database-overflow

Use this command to limit the size of OSPF link state database overflow, a condition where the router is unable to maintain the database in its entirety.

Syntax

database-overflow external {[**exit-overflow-interval** *interval*] [**limit** *limit*] [**warning-level** *level*]}

no database-overflow external {[**exit-overflow-interval** *interval*] [**limit** *limit*] [**warning-level** *level*]}

Parameters

external	Specifies the LSA type as external (Type 5.)
exit-overflow-interval *interval*	Specifies an interval (in seconds) the OSPF link state database will be checked to determine if the overflow limit has been reached. Valid values are **0** - **86400**. Default is **0**.
limit *limit*	Specifies the peak number of LSAs accepted before overflow occurs. Valid values are **0** - **4000**. Default is **0**. **Note:** Limit value must be greater than the warning-level value and set prior to it since all defaults are 0.
warning-level *level*	Specifies the number of LSAs at which a warning of pending overflow will be generated. Valid values are **0** - **4000**. Default is **0**.

Defaults

None.

Downloaded from www.Manualslib.com manuals search engine

Mode

Router command, Router configuration: **Matrix->Router(config-router)#**

Usage

Setting database overflow allows you to set a limit on the number of external LSAs. If the limit is exceeded, self-originated external LSAs will be removed so that OSPF can handle the large number of external LSAs coming from another router. When the warning level is set, a Syslog message will be issued when the number of external LSAs has reached the specified level. Every **exit-overflow interval** seconds, the database will be checked and, if the total is less than the limit specified, the self originated external LSAs will be restored.

The "no" form of this command removes the database overflow limits.

Example

This example shows how to set the OSPF database exit overflow interval to 240 seconds, the overflow limit to 3800 LSAs, and the warning level to 2500 LSAs:

```
Matrix->Router(config)#router ospf 1
Matrix->Router(config-router)#database-overflow external exit-overflow-interval
240
Matrix->Router(config-router)#database-overflow external limit 3800
Matrix->Router(config-router)#database-overflow external warning-level 2500
```

graceful-restart enable

Use this command to enable the graceful-restart ability on this router.

Syntax

graceful-restart enable

no graceful-restart enable

Parameters

None.

Defaults

Disabled.

Mode

Router command, Router configuration: **Matrix->Router(config-router)#**

Usage

Graceful restart allows this router to stay on the forwarding path during a restart of OSPF software. For more information about graceful restart, see "Understanding Graceful Restart" on page 21-19.

The "no" form of this command disables graceful-restart for this router.

Downloaded from www.Manualslib.com manuals search engine

Example

This example shows how to enable the graceful restart ability on this router:

```
Matrix->Router(config)#router ospf 1
Matrix->Router(config-router)#graceful-restart enable
Matrix->Router(config-router)
```

graceful-restart helper-disable

Use this command to disable the graceful restart helper function on this router.

Syntax

graceful-restart helper-disable

no graceful-restart helper-disable

Parameters

None.

Defaults

Helper mode enabled.

Mode

Router command, Router configuration: **Matrix->Router(config-router)#**

Usage

Each restarting router network segment functions as a helper by monitoring the network for topology changes. So long as the helper does not see an LSA change, it continues to advertise its LSAs as though the restarting router remained in continuous operation. This command disables this capability. For more information on the graceful restart helper function, see "Understanding Graceful Restart" on page 21-19.

The "no" form of this command enables graceful-restart helper mode for this router.

Example

This example shows how to disable the helper function on this router:

```
Matrix->Router(config)#router ospf 1
Matrix->Router(config-router)#graceful-restart helper-disable
```

graceful-restart restart-interval

Use this command to set the graceful-restart restart interval.

Syntax

graceful-restart restart-interval *interval*

no graceful-restart restart-interval *interval*

Downloaded from www.Manualslib.com manuals search engine

Parameters

interval	Specifies the maximum amount of time in seconds that this router will remain in graceful-restart mode starting at the time it enters graceful-restart. Valid values are **1** - **1800** seconds. Default value is **120** seconds.

Defaults

None.

Mode

Router command, Router configuration: **Matrix->Router(config-router)#**

Usage

The restart inteval sets the maximum amount of time that this router will remain in graceful restart once an OSPF restart is initiated.

The "no" form of this command resets the graceful-restart restart-interval to its default value.

Example

This example sets the graceful restart restart-interval to 300 seconds:

```
Matrix->Router(config)#router ospf 1
Matrix->Router(config-router)#graceful-restart enable
Matrix->Router(config-router)#graceful-restart restart-interval 300
```

graceful-restart strict-lsa-checking-disable

Use this command to disable strict LSA checking during graceful restart.

Syntax

graceful-restart strict-lsa-checking-disable

no graceful-restart strict-lsa-checking-disable

Parameters

None.

Defaults

Strict LSA checking enabled.

Mode

Router command, Router configuration: **Matrix->Router(config-router)#**

Usage

Strict LSA checking assures that graceful restart will terminate if there is a changed LSA on the restarting router's retransmission list when graceful restart intitiates or an LSA change occurs during graceful restart. With strict LSA checking disabled, graceful restart does not terminate for these conditions.

The "no" form of this command enables strict LSA checking.

Downloaded from www.Manualslib.com manuals search engine

Example

This example shows how to disable strict LSA checking on this router:

```
Matrix->Router(config)#router ospf 1
Matrix->Router(config-router)#graceful-restart strict-lsa-checking-disable
```

show ip ospf

Use this command to display OSPF information.

Syntax

show ip ospf

Parameters

None.

Defaults

None.

Mode

Router command, Any router mode.

Example

This example shows how to display OSPF information:

```
Matrix>Router#show ip ospf
Routing Process "ospf 20 " with ID 134.141.7.2
Supports only single TOS(TOS0) route
It is an area border and autonomous system boundary router
Summary Link update interval is 0 seconds.
External Link update interval is 0 seconds.
Redistributing External Routes from,
Number of areas in this router is 3
Area BACKBONE (0)
    Number of interfaces in this area is 0
    Area has no authentication
    SPF algorithm executed 65 times
    Area ranges are

    Link State Update Interval is 00:30:00 and due in 00:03:12.
    Link State Age Interval is 00:00:00 and due in 00:00:00.

Area 0.0.0.3
    Number of interfaces in this area is 1
    Area has no authentication
    SPF algorithm executed 59 times
    Area ranges are
```


Downloaded from www.Manualslib.com manuals search engine

```
    Link State Update Interval is 00:30:00 and due in 00:02:28.
    Link State Age Interval is 00:00:00 and due in 00:00:00.

Area 0.0.0.2
    Number of interfaces in this area is 3
    Area has no authentication
    SPF algorithm executed 61 times
    Area ranges are
         140.20.0.0/255.255.0.0

    Link State Update Interval is 00:30:00 and due in 00:03:07.
    Link State Age Interval is 00:00:00 and due in 00:00:00.
```

show ip ospf database

Use this command to display the OSPF link state database.

Syntax

show ip ospf database [*link-state-id*]

The options for using this syntax are:

show ip ospf database router [*link-state-id*]

show ip ospf database network [*link-state-id*]

show ip ospf database summary [*link-state-id*]

show ip ospf database asbr-summary [*link-state-id*]

show ip ospf database external [*link-state-id*]

show ip ospf database nssa-external [*link-state-id*]

show ip ospf database database-summary

Parameters

link-state-id	(Optional) Specifies the link state identifier. Valid values are IP addresses.
router	Displays router (Type 1) link state records in their detailed format. Router records are originated by all routers.
network	Displays network (Type 2) link state records in their detailed format. Network records are originated by designated routers.
summary	Displays summary (Type 3) link state records in their original format. Summary records are originated by ABRs.
asbr-summary	Displays Autonomous System Border Router (ASBR) summary (Type 4) link status records in their detail format. ASBR-summary records are originated by ABRs.
external	Displays external (Type 5) link state records. Type 5 link state records in their detailed format.

Downloaded from www.Manualslib.com manuals search engine

nssa-external	Displays nssa-external (Type 7) link state records in their detailed format. Type 7 records are originated by ASBRs.
database-summary	Displays a numerical summary of the contents of the link state database.

Defaults

If *link-state-id* is not specified, the specified type of database records will be displayed for all link state IDs.

Mode

Router command, Any router mode.

Example

This example shows how to display all OSPF link state database information:

```
Matrix>Router#show ip ospf database
OSPF Router with ID(182.127.64.1)

         Displaying Net Link States(Area 0.0.0.0)
 LinkID         ADV Router      Age       Seq#      Checksum
182.127.63.1    182.127.62.1    956  0x80000001     0xb6ca

         Displaying Router Link States(Area 0.0.0.0)
 LinkID         ADV Router      Age       Seq#      Checksum LinkCount
182.127.64.1    182.127.64.1    308  0x8000000f     0x636b     2
182.127.62.1    182.127.62.1    952  0x8000001b     0x7ed7     1

         Displaying Summary Net Link States(Area 0.0.0.0)
 LinkID         ADV Router      Age       Seq#      Checksum
182.127.63.1    182.127.62.1    956  0x80000001     0xb6ca
```

Table 21-3 provides an explanation of the command output.

Table 21-3 show ip ospf database Output Details

Output...	What it displays...
Link ID	Link ID, which varies as a function of the link state record type, as follows: • Net Link States - Shows the interface IP address of the designated router to the broadcast network. • Router Link States - Shows the ID of the router originating the record. • Summary Link States - Shows the summary network prefix.
ADV Router	Router ID of the router originating the link state record.
Age	Age (in seconds) of the link state record.
Seq#	OSPF sequence number assigned to each link state record.

Downloaded from www.Manualslib.com manuals search engine

Table 21-3 show ip ospf database Output Details (continued)

Output...	What it displays...
Checksum	Field in the link state record used to verify the contents upon receipt by another router.
LinkCount	Link count of router link state records. This number is equal to, or greater than, the number of active OSPF interfaces on the originating router.

show ip ospf border-routers

Use this command to display information about OSPF internal entries to Area Border Routers (ABRs) and Autonomous System Boundary Routers (ASBRs).

Syntax

show ip ospf border-routers

Parameters

None.

Defaults

None.

Mode

Router command, Any router mode.

Example

This example shows how to display information about OSPF border routers. The first line of this output shows that an intra-area route has been established to destination border router 192.168.22.1 via neighboring router 192.168.11.1 on the VLAN 2 interface in area 0. The OSPF cost of this route is 64, and it carries an SPF calculation of 10. The destination router is an ABR:

```
Matrix>Router#show ip ospf border-routers
OSPF internal
Codes: i - Intra-area route, I - Inter-area route
i 192.168.22.1 [64] via 192.168.11.1, VLAN2, ABR, Area 0, SPF 10
i 192.168.22.1 [64] via 192.168.11.1, VLAN2, ABR, Area 4, SPF 10
i 192.168.44.1 [64] via 192.168.33.1, VLAN1, ABR, Area 0, SPF 10
i 192.168.44.1 [64] via 192.168.33.1, VLAN1, ABR, Area 2, SPF 7
i 192.168.44.2 [128] via 192.168.33.1, VLAN1, ABR, Area 0, SPF 10
i 192.168.44.2 [128] via 192.168.11.1, VLAN2, ABR, Area 0, SPF 10
```

show ip ospf interface

Use this command to display OSPF interface related information, including network type, priority, cost, hello interval, and dead interval.

Syntax

show ip ospf interface [**vlan** *vlan-id*]

Downloaded from www.Manualslib.com manuals search engine

Parameters

vlan *vlan-id*	(Optional) Displays OSPF information for a specific VLAN. This VLAN must be configured for IP routing as described in "Pre-Routing Configuration Tasks" on page 2-100.

Defaults

If *vlan-id* is not specified, OSPF statistics will be displayed for all VLANs.

Mode

Router command, Any router mode.

Example

This example shows how to display all OSPF related information for VLAN 1:

```
Matrix>Router#show ip ospf interface vlan 1
Vlan  1 is UP
 Internet Address  182.127.63.2  Mask  255.255.255.0,Area 0.0.0.0
 Router ID 182.127.64.1,Network Type BROADCAST,Cost: 10
 Transmit Delay is 1 sec,State BACKUPDR,Priority 1
 Designated Router id 182.127.62.1, Interface addr 182.127.63.1
 Backup Designated Router id 182.127.63.2,
 Timer intervals configured, Hello 10,Dead 40,Wait 40,Retransmit 5
    Neighbor Count is 1, Adjacent neighbor count is 1
  Adjacent with neighbor 182.127.63.1 (Designated Router)
```

Table 21-4 provides an explanation of the command output.

Table 21-4 show ip ospf interface Output Details

Output...	What it displays...
Vlan	Interface (VLAN) administrative status as up or down.
Internet Address	IP address and mask assigned to this interface.
Router ID	Router ID, which OSPF selects from IP addresses configured on this router.
Network Type	OSPF network type, for instance, broadcast.
Cost	OSPF interface cost, which is either default, or assigned with the **ip ospf cost** command. For details, refer to "ip ospf cost" on page 21-24.
Transmit Delay	The number (in seconds) added to the LSA (Link State Advertisement) age field.
State	The interface state (versus the state between neighbors). Valid values include BACKUPDR (Backup Designated Router), and DR (Designated Router).
Priority	The interface priority value, which is either default, or assigned with the **ip ospf priority** command. For details, refer to "ip ospf priority" on page 21-25.
Designated Router id	The router ID of the designated router on this subnet, if one exists.
Interface addr	IP address of the designated router on this interface.
Backup Designated Router id	IP address of the backup designated router on this interface, if one exists.

Downloaded from www.Manualslib.com manuals search engine

Table 21-4 show ip ospf interface Output Details (continued)

Output...	What it displays...
Timer intervals configured	OSPF timer intervals. These are either default, or configured with the **ip ospf retransmit-interval** ("ip ospf retransmit-interval" on page 21-26), the **ip ospf hello-interval** ("ip ospf hello-interval" on page 21-28), and the **ip ospf dead interval** ("ip ospf dead-interval" on page 21-28) commands. The wait timer represents the amount of time a router waits before initiating a designated router/backup designated router election. The wait timer changes when the dead interval changes. The retransmit timer represents the amount of time between successive transmissions of LSAs (Link State Advertisements) until acknowledgement is received.
Neighbor Count	Number of neighbors over this interface.
Adjacent neighbor count	Number of adjacent (FULL state) neighbors over this interface.
Adjacent with neighbor	IP address of the adjacent neighbor.

show ip ospf neighbor

Use this command to display the state of communication between an OSPF router and its neighbor routers.

Syntax

show ip ospf neighbor [**detail**] [*ip-address*] [**vlan** *vlan-id*]

Parameters

detail	(Optional) Displays detailed information about the neighbors, including the area in which they are neighbors, who the designated router/backup designated router is on the subnet, if applicable, and the decimal equivalent of the E-bit value from the hello packet options field.
ip-address	(Optional) Displays OSPF neighbors for a specific IP address.
vlan *vlan*-id	(Optional) Displays OSPF neighbors for a specific VLAN. This VLAN must be configured for IP routing as described in "Pre-Routing Configuration Tasks" on page 2-100.

Defaults

- If **detail** is not specified, summary information will be displayed.
- If *ip-address* is not specified, OSPF neighbors will be displayed for all IP addresses configured for routing.
- If *vlan-id* is not specified, OSPF neighbors will be displayed for all VLANs configured for routing.

Mode

Router command, Any router mode.

Downloaded from www.Manualslib.com manuals search engine

Example

This example shows how to use the **show ospf neighbor** command:

```
Matrix>Router#show ip ospf neighbor
ID              Pri     State     Dead-Int  Address       Interface
182.127.62.1      1     FULL      40        182.127.63.1  vlan1
```

Table 21-5 provides an explanation of the command output.

Table 21-5 show ip ospf neighbor Output Details

Output...	What it displays...
ID	Neighbor's router ID of the OSPF neighbor.
Pri	Neighbor's priority over this interface.
State	Neighbor's OSPF communication state.
Dead-Int	Interval (in seconds) this router will wait without receiving a Hello packet from a neighbor before declaring the neighbor is down.
Address	Neighbor's IP address.
Interface	Neighbor's interface (VLAN).

show ip ospf virtual-links

Use this command to display information about the virtual links configured on a router.

Syntax

show ip ospf virtual-links

Parameters

None.

Defaults

None.

Mode

Router command, Any router mode.

Usage

A virtual link represents a logical connection between the backbone and a non-backbone OSPF area.

Example

This example shows how to display OSPF virtual links information:

```
Matrix>Router#show ip ospf virtual-links
Virtual Link to router 5.5.5.1, is UP
 Transit area 0.0.0.2,via interface Vlan 7, Cost of using 10
 Transmit Delay is 1 sec(s), State POINT-TO-POINT
 Timer intervals configured:
```


Downloaded from www.Manualslib.com manuals search engine

```
                Hello 10, Dead 40, Wait 40, Retransmit 5
 Adjacency State FULL
```

Table 21-6 provides an explanation of the command output.

Table 21-6 show ip ospf virtual links Output Details

Output...	What it displays...
Virtual Link	ID of the virtual link neighbor, and the virtual link status, which is up or down.
Transit area	ID of the transit area through which the virtual link is configured.
via interface	Router's interface into the transit area.
Cost of using	OSPF cost of routing through the virtual link.
Transit Delay	Time (in seconds) added to the LSA (Link State Advertisement) age field when the LSA is transmitted through the virtual link.
State	Interface state assigned to a virtual link, which is point-to-point.
Timer intervals configured	Timer intervals configured for the virtual link, including Hello, Dead, Wait, and Retransmit intervals.
Adjacency State	State of adjacency between this router and the virtual link neighbor of this router.

clear ip ospf process

Use this command to reset the OSPF process.

Syntax

clear ip ospf process *process-id*

Parameters

process-id	Specifies the process ID, an internally used identification number for each instance of the OSPF routing process run on a router. Valid values are **1** to **65535**.

Defaults

None.

Mode

Router command, Privileged EXEC: **Matrix>Router#**

Usage

This command will require adjacencies to be reestablished and routes to be reconverged.

Example

This example shows how to reset OSPF process 1:

```
Matrix>Router#clear ip ospf process 1
```


Downloaded from www.Manualslib.com manuals search engine

debug ip ospf

Use this command to enable OSPF protocol debugging output.

Syntax

debug ip ospf {*subsystem*}

no debug ip ospf {*subsystem*}

Parameters

subsystem	Specifies the OSPF subsystem for which protocol debugging will be enabled. Valid entries and their associated outputs are: • **adj** - OSPF adjacency events • **flood** - OSPF flooding • **lsa-generation** - OSPF Link State Advertisement generation • **packet** - OSPF packets • **retransmission** - OSPF retransmission events

Defaults

None.

Mode

Router command, Privileged EXEC: **Matrix>Router#**

Usage

The “no” form of this command disables OSPF protocol debugging output.

Example

This example shows how to enable OSPF protocol debugging output to display information about Link State Advertisement generation:

```
Matrix>Router#debug ip ospf lsa-generation
```

rfc1583compatible

Use this command to enable the OSPF router for RFC 1583 compatibility.

Syntax

rfc1583compatible

no rfc1583compatible

Parameters

None.

Defaults

None.

Downloaded from www.Manualslib.com manuals search engine

Mode

Router command, Router configuration: **Matrix>Router(config-router)#**

Usage

The "no" form of this command removes OSPF RFC 1583 compatible.

Example

This example shows how to configure RFC 1583 compatibility:

```
Matrix>Router(config)#router ospf 1
Matrix>Router(config-router)#rfc1583compatible
```


Downloaded from www.Manualslib.com manuals search engine

Configuring DVMRP

Purpose

To enable and configure the Distance Vector Multicast Routing Protocol (DVMRP) on an interface. DVMRP routes multicast traffic using a technique known as Reverse Path Forwarding. When a router receives a packet, it floods the packet out of all paths except the one that leads back to the packet's source. Doing so allows a data stream to reach all VLANs (possibly multiple times). If a router is attached to a set of VLANs that do not want to receive from a particular multicast group, the router can send a "prune" message back up the distribution tree to stop subsequent packets from traveling where there are no members. DVMRP will periodically reflood in order to reach any new hosts that want to receive from a particular group.



Note: IGMP must be enabled on all VLANs running DVMRP. To do this, use the **set igmp enable** command as described in "set igmp enable" on page 9-3. It is also recommended that IGMP querying be enabled on all VLANs running DVMRP. To do this, use the **set igmp query-enable** command as described in "set igmp query-enable" on page 9-6.

Commands

For information about...	Refer to page...
ip dvmrp	21-52
ip dvmrp metric	21-53
show ip dvmrp route	21-53

ip dvmrp

Use this command to enable or disable DVMRP on an interface.

Syntax

```
ip dvmrp
no ip dvmrp
```

Parameters

None.

Defaults

None.

Mode

Router command, Interface configuration: **Matrix>Router(config-if(Vlan 1))#**

Usage

IGMP must be enabled on all VLANs running DVMRP. To do this, use the **set igmp enable** command as described in "set igmp enable" on page 9-3. It is also recommended that IGMP querying be enabled on all VLANs running DVMRP. To do this, use the **set igmp query-enable** command as described in "set igmp query-enable" on page 9-6.

Downloaded from www.Manualslib.com manuals search engine

The “no” form of this command disables DVMRP.

Example

This example shows how to enable DVMRP on VLAN 1:

```
Matrix>Router(config)#interface vlan 1
Matrix>Router(config-if(Vlan 1))#ip dvmrp
```

ip dvmrp metric

Use this command to configure the metric associated with a set of destinations for DVMRP reports.

Syntax

ip dvmrp metric *metric*

Parameters

metric	Specifies a metric associated with a set of destinations for DVMRP reports. Valid values are from **0** to **31**. Entering a **0** value will reset the metric back to the default value of 1.

Defaults

None.

Mode

Router command, Interface configuration: **Matrix>Router(config-if(Vlan 1))#**

Usage

To reset the DVMRP metric back to the default value of 1, enter **ip dvmrp metric 0**.

Example

This example shows how to set a DVMRP of 16 on VLAN 1:

```
Matrix>Router(config-if(Vlan 1))#ip dvmrp metric 16
```

show ip dvmrp route

Use this command to display DVMRP routing information.

Syntax

show ip dvmrp route

Parameters

None.

Defaults

None.

Downloaded from www.Manualslib.com manuals search engine

Mode

Router command, Any router mode.

Example

This example shows how to display DVMRP routing table entries. In this case, the routing table has 5 entries. The first entry shows that the source network 60.1.1.0/24 can be reached via next-hop router 40.1.1.3. This route has a metric of 2. It has been in the DVMRP routing table for 1 hour, 24 minutes and 2 seconds and will expire in 2 minutes and 3 seconds. It supports flag messages for verifying neighbors, pruning, generation ID and netmask in prunes and grafts (VPGN):

```
Matrix>Router#show ip dvmrp route
flag characters used:
-------------
V Neighbor is verified.
P Neighbor supports pruning.
G Neighbor supports generation ID.
N Neighbor supports netmask in prunes and grafts.
S Neighbor supports SNMP.
M Neighbor supports mtrace.
----------------
DVMRP Routing Table - 5 entries
60.1.1.0/24 [2] uptime: 1:24:2, expires: 0:2:3
    via neighbor: 40.1.1.3 version: 3.255  flags: VPGN  gen id: 0x336ff052
50.50.50.0/24 [2] uptime: 1:24:18, expires: 0:1:25
    via neighbor: 30.1.1.1 version: 3.255  flags: VPGN  gen id: 0xaa4ee1fa
40.40.40.0/24 [2] uptime: 1:24:2, expires: 0:2:3
   via neighbor: 40.1.1.3 version: 3.255  flags: VPGN  gen id: 0x336ff052 40.1.1.0/
24 [1] uptime: 1:24:8, expires: 0:0:0
    via: local
30.1.1.0/24 [1] uptime: 1:24:20, expires: 0:0:0
    via: local
```


Downloaded from www.Manualslib.com manuals search engine

Configuring IRDP

Purpose

To enable and configure the ICMP Router Discovery Protocol (IRDP) on an interface. This protocol enables a host to determine the address of a router it can use as a default gateway.

Commands

For information about...	Refer to page...
ip irdp	21-55
ip irdp maxadvertinterval	21-56
ip irdp minadvertinterval	21-56
ip irdp holdtime	21-57
ip irdp preference	21-58
ip irdp address	21-58
no ip irdp multicast	21-59
show ip irdp	21-59

ip irdp

Use this command to enable or disable IRDP on an interface.

Syntax

ip irdp

no ip irdp

Parameters

None.

Defaults

None.

Mode

Router command, Interface configuration: **Matrix>Router(config-if(Vlan 1))#**

Usage

The “no” form of this command disables IRDP on an interface.

Example

This example shows how to enable IRDP on VLAN 1:

```
Matrix>Router(config)#interface vlan 1
Matrix>Router(config-if(Vlan 1))#ip irdp
```


Downloaded from www.Manualslib.com manuals search engine

ip irdp maxadvertinterval

Use this command to set the maximum interval in seconds between IRDP advertisements.

Syntax

ip irdp maxadvertinterval *interval*

no irdp maxadvertinterval

Parameters

interval	Specifies a maximum advertisement interval in seconds. Valid values are **4** to **1800**. Default: **600** Seconds.

Defaults

None.

Mode

Router command, Interface configuration: **Matrix>Router(config-if(Vlan 1))#**

Usage

The "no" form of this command resets the maximum advertisement interval to the default value.

Example

This example shows how to set the maximum IRDP advertisement interval to 1000 seconds on VLAN 1:

```
Matrix>Router(config)#interface vlan 1
Matrix>Router(config-if(Vlan 1))#ip irdp maxadvertinterval 1000
```

ip irdp minadvertinterval

Use this command to set the minimum interval in seconds between IRDP advertisements.

Syntax

ip irdp minadvertinterval *interval*

no irdp minadvertinterval

Parameters

interval	Specifies a minimum advertisement interval in seconds. Valid values are **3** to **1800**.

Defaults

None.

Mode

Router command, Interface configuration: **Matrix>Router(config-if(Vlan 1))#**

Downloaded from www.Manualslib.com manuals search engine

Usage

The "no" form of this command deletes the custom holdtime setting and resets the minimum advertisement interval to the default value of three-fourths of the **maxadvertinterval** value.

Example

This example shows how to set the minimum IRDP advertisement interval to 500 seconds on VLAN 1:

```
Matrix>Router(config)#interface vlan 1
Matrix>Router(config-if(Vlan 1))#ip irdp minadvertinterval 500
```

ip irdp holdtime

Use this command to set the length of time in seconds IRDP advertisements are held valid.

Syntax

ip irdp holdtime *holdtime*

no irdp holdtime

Parameters

holdtime	Specifies the hold time in seconds. Valid values are **0** to **9000**.

Defaults

None.

Mode

Router command, Interface configuration: **Matrix>Router(config-if(Vlan 1))#**

Usage

Hold time is automatically set at three times the **maxadvertinterval** value when the maximum advertisement interval is set as described in "ip irdp maxadvertinterval" on page 21-56 and the minimum advertisement interval is set as described in "ip irdp minadvertinterval" on page 21-56.

The "no" form of this command resets the hold time to the default value of three times the **maxadvertinterval** value.

Example

This example shows how to set the IRDP hold time to 4000 seconds on VLAN 1:

```
Matrix>Router(config)#interface vlan 1
Matrix>Router(config-if(Vlan 1))#ip irdp holdtime 4000
```


Downloaded from www.Manualslib.com manuals search engine

ip irdp preference

Use this command to set the IRDP preference value for an interface. This value is used by IRDP to determine the interface's selection as a default gateway address.

Syntax

ip irdp preference *preference*

no irdp preference

Parameters

preference	Specifies the value to indicate the interface's use as a default router address. Valid values are **-2147483648** to **2147483647**. The value of **80000000** indicates that the address, even though it may be advertised, is not to be used by neighboring hosts as a default router address.

Defaults

None.

Mode

Router command, Interface configuration: **Matrix>Router(config-if(Vlan 1))#**

Usage

The "no" form of this command resets the interface's IRDP preference value to the default of **0**.

Example

This example shows how to set the IRDP preference value to 80000000 seconds on VLAN 1:

```
Matrix>Router(config)#interface vlan 1
Matrix>Router(config-if(Vlan 1))#ip irdp preference 80000000
```

ip irdp address

Use this command to add additional IP addresses for IRDP to advertise.

Syntax

ip irdp address *ip-address preference*

no ip irdp preference *ip-address*

Parameters

ip-address	Specifies an IP address to advertise.
preference	Specifies the value to indicate the address' use as a default router address. Valid values are **-2147483648** to **2147483647**. The value of **80000000** indicates that the address, even though it may be advertised, is not to be used by neighboring hosts as a default router address.

Defaults

None.

Downloaded from www.Manualslib.com manuals search engine

Mode

Router command, Interface configuration: **Matrix>Router(config-if(Vlan 1))#**

Usage

The "no" form of this command clears an IP address from being advertised.

Example

This example shows how to advertise IP address 183.255.0.162 with a preference of 1 on VLAN 1:

```
Matrix>Router(config)#interface vlan 1
Matrix>Router(config-if(Vlan 1))#ip irdp address 183.255.0.162 1
```

no ip irdp multicast

Use this command to enable the router to send IRDP advertisements using broadcast rather than multicast transmissions. By default, the router sends IRDP advertisements via multicast.

Syntax

no ip irdp multicast

Parameters

None.

Defaults

None.

Mode

Router command, Interface configuration: **Matrix>Router(config-if(Vlan 1))#**

Example

This example shows how to enable the router to send IRDP advertisements using broadcast:

```
Matrix>Router(config)#interface vlan 1
Matrix>Router(config-if(Vlan 1))#no ip irdp multicast
```

show ip irdp

Use this command to display IRDP information.

Syntax

show ip irdp [**vlan** *vlan-id*]

Parameters

vlan *vlan-id*	(Optional) Displays IRDP information for a specific VLAN. This VLAN must be configured for IP routing as described in "Pre-Routing Configuration Tasks" on page 2-100.

Downloaded from www.Manualslib.com manuals search engine

Defaults

If **vlan** *vlan-id* is not specified, IRDP information for all interfaces will be displayed.

Mode

Router command, Interface configuration: **Matrix>Router(config-if(Vlan 1))#**

Example

This example shows how to display IRDP information for VLAN 1:

```
Matrix>Router(config)#interface vlan 1
Matrix>Router(config-if(vlan 1))#show ip irdp vlan 1
Interface 1 is not enabled
```


Downloaded from www.Manualslib.com manuals search engine

Configuring VRRP

Purpose

To enable and configure the Virtual Router Redundancy Protocol (VRRP). This protocol eliminates the single point of failure inherent in the static default routed environment by transferring the responsibility from one router to another if the original router goes down. VRRP-enabled routers decide who will become master and who will become backup in the event the master fails.

Commands

For information about...	Refer to page...
router vrrp	21-61
create	21-62
address	21-63
priority	21-64
master-icmp-reply	21-65
advertise-interval	21-66
critical-ip	21-66
preempt	21-67
preempt-delay	21-68
enable	21-69
ip vrrp authentication-key	21-70
ip vrrp message-digest-key	21-70
show ip vrrp	21-71

router vrrp

Use this command to enable or disable VRRP configuration mode.

Syntax

```
router vrrp
no router vrrp
```

Parameters

None.

Defaults

None.

Mode

Router command, Global configuration: **Matrix>Router(config)#**

Downloaded from www.Manualslib.com manuals search engine

Usage

You must execute the **router vrrp** command to enable the protocol before completing other VRRP-specific configuration tasks. For details on enabling configuration modes, refer to Table 2-8 in "Enabling Router Configuration Modes" on page 2-103.

The "no" form of this command removes all VRRP configurations from the running configuration.

Example

This example shows how enable VRRP configuration mode:

```
Matrix>Router#configure terminal
Matrix>Router(config)#router vrrp
Matrix>Router(config-router)#
```

create

Use this command to create a VRRP session.

Syntax

create vlan *vlan-id vrid*

no create vlan *vlan-id vrid*

Parameters

vlan *vlan-id*	Specifies the number of the VLAN on which to create a VRRP session. This VLAN must be configured for IP routing as described in "Pre-Routing Configuration Tasks" on page 2-100.
vrid	Specifies a unique Virtual Router ID (VRID) to associate with the routing interface. The value of *vrid* can range from 1 to 255.

Defaults

None.

Mode

Router command, Router configuration: **Matrix>Router(config-router)#**

Usage

This command must be executed to create an instance of VRRP on a routing interface (VLAN) before any other VRRP settings can be configured.

Each Enterasys Matrix Series Gold routing module supports up to 128 VRRP sessions. Up to four VRIDs can be associated with an individual routing interface.

The "no" form of this command disables the VRRP session.

Example

This example shows how to create a VRRP session on VLAN 1 with a VRID of 1:

```
Matrix>Router(config)#router vrrp
Matrix>Router(config-router)#create vlan 1 1
```


Downloaded from www.Manualslib.com manuals search engine

address

Use this command to configure a virtual router IP address.

Syntax

address vlan *vlan-id vrid ip-address owner*

no address vlan *vlan-id vrid ip-address owner*

Parameters

vlan *vlan-id*	Specifies the number of the VLAN on which to configure a virtual router address. This VLAN must be configured for IP routing as described in "Pre-Routing Configuration Tasks" on page 2-100.
vrid	Specifies a unique Virtual Router ID (VRID) associated with the routing interface.
ip-address	Specifies the virtual router IP address to associate with the router. The limit is 16 virtual router IP addresses per interface.
owner	Specifies a value to indicate if the router owns the IP address as one of its interfaces. Valid values are: • **1** to indicate the router owns the address. • **0** to indicate the router does not own the address.

Defaults

None.

Mode

Router command, Router configuration: **Matrix>Router(config-router)#**

Usage

If the virtual router IP address is the same as the interface (VLAN) address owned by a VRRP router, then the router owning the address becomes the master. The master sends an advertisement to all other VRRP routers declaring its status and assumes responsibility for forwarding packets associated with its virtual router ID (VRID).

If the virtual router IP address is not owned by any of the VRRP routers, then the routers compare their priorities and the higher priority owner becomes the master. If priority values are the same, then the VRRP router with the higher IP address is selected master. For details on using the **priority** command, refer to "priority" on page 21-64.

Each VRRP routing interface can support up to 16 virtual router IP addresses. A virtual router IP address can be either an address configured on the routing interface or an address that falls within the range of any networks configured on the routing interface. All of the virtual router IP addresses associated with a single VRID must be designated as "owner" or "non-owner"— a mix of "owner" and "non-owner" addresses on a single VRID is not allowed.

The "no" form of this command clears the VRRP address configuration.

Downloaded from www.Manualslib.com manuals search engine

Examples

This example shows how to configure a virtual router address of 182.127.62.1 on VLAN 1, VRID 1, and to set the router connected to the VLAN via this interface as the master:

```
Matrix>Router(config)#router vrrp
Matrix>Router(config-router)#address vlan 1 1 182.127.62.1 1
```

This example shows how to configure 5 virtual router addresses on a single interface, VLAN 1, VRID 1. All 5 addresses fall within the range of networks configured on the VLAN 1 routing interface, because VLAN 1 has a primary IP address of 182.127.62.1/24, and secondary IP addresses of 10.1.1.1/24 and 10.2.2.1/24. All virtual addresses are non-owners.

```
Matrix>Router(config)#router vrrp
Matrix>Router(config-router)#address vlan 1 1 182.127.62.2 0
Matrix>Router(config-router)#address vlan 1 1 10.1.1.2 0
Matrix>Router(config-router)#address vlan 1 1 10.1.1.3 0
Matrix>Router(config-router)#address vlan 1 1 10.2.2.2 0
Matrix>Router(config-router)#address vlan 1 1 10.2.2.3 0
```

priority

Use this command to set a priority value for a VRRP router.

Syntax

priority vlan *vlan-id vrid priority-value*

no priority vlan *vlan-id vrid priority-value*

Parameters

vlan *vlan-id*	Specifies the number of the VLAN on which to configure VRRP priority. This VLAN must be configured for IP routing as described in "Reviewing and Configuring Routing" on page 2-101.
vrid	Specifies a unique Virtual Router ID (VRID) associated with the routing interface. Valid values are from **1** to **255**.
priority-value	Specifies the VRRP priority value to associate with the *vrid*. Valid values are from **1** to **254**, with the highest value setting the highest priority. Priority value of **255** is reserved for the VRRP router that owns the IP address associated with the virtual router. Priority **0** is reserved for signaling that the master has stopped working and the backup router must transition to master state.

Defaults

None.

Mode

Router command, Router configuration: **Matrix>Router(config-router)#**

Usage

The "no" form of this command clears the VRRP priority configuration.

Downloaded from www.Manualslib.com manuals search engine

Example

This example shows how set a VRRP priority of 200 on VLAN 1, VRID 1:

```
Matrix>Router(config)#router vrrp
Matrix>Router(config-router)#priority vlan 1 1 200
```

master-icmp-reply

Use this command to enable ICMP replies for non-owner masters.

Syntax

master-icmp-reply vlan *vlan-id vrid*

no master-icmp-reply vlan *vlan-id vrid*

Parameters

vlan *vlan-id*	Specifies the number of the VLAN on which to enable master ICMP replies. This VLAN must be configured for IP routing as described in "Reviewing and Configuring Routing" on page 2-101.
vrid	Specifies a unique Virtual Router ID (VRID) associated with the routing interface. Valid values are from **1** to **255**.

Defaults

None.

Mode

Router command, Router configuration: **Matrix>Router(config-router)#**

Usage

This command provides the ability for the virtual router master to respond to an ICMP echo even if it does not "own" the virtual IP address. Without this function, the virtual router can only respond to an ICMP echo when the virtual IP address matches the real IP address of the interface. Therefore, when the backup router takes over, there would be no device that would answer the ICMP echo for that virtual IP (because only the primary was configured with the matching real IP). With master-icmp-reply enabled, management stations that use "ping" to poll devices will be able to "see" that the virtual router is available when the backup router assumes the role of master.

The "no" form of this command disables master ICMP replies.

Example

This example shows how enable master ICMP replies on VLAN 1, VRID 1:

```
Matrix>Router(config)#router vrrp
Matrix>Router(config-router)#master-icmp-reply vlan 1 1
```


Downloaded from www.Manualslib.com manuals search engine

advertise-interval

Use this command to set the interval in seconds between VRRP advertisements.

Syntax

advertise-interval vlan *vlan-id vrid interval*

no advertise-interval vlan *vlan-id vrid interval*

Parameters

vlan *vlan-id*	Specifies the number of the VLAN on which to configure the VRRP advertisement interval. This VLAN must be configured for IP routing as described in "Reviewing and Configuring Routing" on page 2-101.
vrid	Specifies a unique Virtual Router ID (VRID) associated with the routing interface. Valid values are from **1** to **255**.
interval	Specifies a VRRP advertisement interval to associate with the *vrid*. Valid values are from **1** to **255** seconds.

Defaults

None.

Mode

Router command, Router configuration: **Matrix>Router(config-router)#**

Usage

All routers with the same VRID should be configured with the same advertisement interval.

VRRP advertisements are sent by the master router to other routers participating in the VRRP master selection process, informing them of its configured values. Once the master is selected, then advertisements are sent every advertising interval to let other VRRP routers in this VLAN/VRID know the router is still acting as master of the VLAN/VRID.

The "no" form of this command clears the VRRP advertise interval value.

Example

This example shows how set an advertise interval of 3 seconds on VLAN 1, VRID 1:

```
Matrix>Router(config)#router vrrp
Matrix>Router(config-router)#advertise-interval vlan 1 1 3
```

critical-ip

Use this command to set a critical IP address for VRRP routing.

Syntax

critical-ip vlan *vlan-id vrid ip-address* [*critical-priority*]

no critical-ip vlan *vlan-id vrid ip-address*

Downloaded from www.Manualslib.com manuals search engine

Parameters

vlan *vlan-id*	Specifies the number of the VLAN on which to set the critical IP address. This VLAN must be configured for IP routing as described in "Reviewing and Configuring Routing" on page 2-101.
vrid	Specifies a unique Virtual Router ID (VRID) associated with the routing interface. Valid values are from **1** to **255**.
ip-address	Specifies the IP address to set as the critical IP address.
critical-priority	(Optional) Specifies the value by which the VRID's priority will decrease as a critical IP becomes unavailable.

Defaults

If not specified, *critical-priority* will be set to 10.

Mode

Router command, Router configuration: **Matrix>Router(config-router)#**

Usage

A critical IP address defines an interface — in addition to the interface between hosts and a first-hop router — that will prevent the master router from functioning properly if the interface were to fail. For example, an IP address of an interface connecting a master router to a router configured for internet access would be considered a critical IP address for VRRP routing. Up to four critical IP addresses can be configured on the device.

The "no" form of this command clears the critical IP address.

Example

This example shows how to set IP address 182.127.62.3 as a critical IP address associated with VLAN 1, VRID 1:

```
Matrix>Router(config)#router vrrp
Matrix>Router(config-router)#critical-ip vlan 1 1 182.127.62.3
```

preempt

Use this command to enable or disable preempt mode on a VRRP router.

Syntax

preempt *vlan-id vrid*

no preempt *vlan-id vrid*

Parameters

vlan *vlan-id*	Specifies the number of the VLAN on which to set preempt mode. This VLAN must be configured for IP routing as described in "Reviewing and Configuring Routing" on page 2-101.
vrid	Specifies a unique Virtual Router ID (VRID) associated with the routing interface. Valid values are from **1** to **255**.

Downloaded from www.Manualslib.com manuals search engine

Defaults

None.

Mode

Router command, Router configuration: **Matrix>Router(config-router)#**

Usage

The router that owns the virtual router IP address always preempts other routers, regardless of this setting.

Preempt is enabled on VRRP routers by default, which allows a higher priority backup router to preempt a lower priority master.

The "no" form of this command disables preempt mode.

Example

This example shows how to disable preempt mode on VLAN 1, VRID 1:

```
Matrix>Router(config)#router vrrp
Matrix>Router(config-router)#no preempt vlan 1 1
```

preempt-delay

Use this command to set a preempt delay time on a VRRP router.

Syntax

preempt-delay *vlan-id vrid delay-timer*

no preempt-delay *vlan-id vrid*

Parameters

vlan *vlan-id*	Specifies the number of the VLAN on which to set a preempt delay value. This VLAN must be configured for IP routing as described in "Reviewing and Configuring Routing" on page 2-101, and must have preempt mode enabled as described in "preempt" on page 21-67.
vrid	Specifies a unique Virtual Router ID (VRID) associated with the routing interface. Valid values are from **1** to **255**.
delay-timer	Specifies a preempt delay time in seconds. Valid values are from **1** to **900**.

Defaults

None.

Mode

Router command, Router configuration: **Matrix>Router(config-router)#**

Usage

The router that owns the virtual router IP address always preempts other routers, regardless of this setting.

Downloaded from www.Manualslib.com manuals search engine

When preempt mode is enabled this specifies a delay (in seconds) that a higher priority backup router must wait to preempt a lower priority master. For more information on setting preempt status, refer back to "preempt" on page 21-67. For more information on setting VRRP priority, refer back to "priority" on page 21-64.

The "no" form of this command clears the preempt delay timer.

Example

This example shows how to set the preempt delay to 60 seconds on VLAN 1, VRID 1:

```
Matrix>Router(config)#router vrrp
Matrix>Router(config-router)#preempt-delay vlan 1 1 60
```

enable

Use this command to enable VRRP on an interface.

Syntax

enable vlan *vlan-id vrid*

no enable vlan *vlan-id vrid*

Parameters

vlan *vlan-id*	Specifies the number of the VLAN on which to enable VRRP. This VLAN must be configured for IP routing as described in "Reviewing and Configuring Routing" on page 2-101.
vrid	Specifies the Virtual Router ID (VRID) associated with the *vlan-id*. Valid values are from **1** to **255**.

Defaults

None.

Mode

Router command, Router configuration: **Matrix>Router(config-router)#**

Usage

Before enabling VRRP, you must set the other options described in this section. Once enabled, you cannot make any configuration changes to VRRP without first disabling it using the **no enable vlan** command.

The "no" form of this command disables VRRP on an interface.

Example

This example shows how to enable VRRP on VLAN 1, VRID 1:

```
Matrix>Router(config)#router vrrp
Matrix>Router(config-router)#enable vlan 1 1
```


Downloaded from www.Manualslib.com manuals search engine

ip vrrp authentication-key

Use this command to set a VRRP authentication password on an interface.

Syntax

ip vrrp authentication-key *password*

no ip vrrp authentication-key

Parameters

password	Specifies an authentication password. Text string can be 1 to 8 characters in length.

Defaults

None.

Mode

Router command, Interface configuration: **Matrix>Router(config-if(Vlan 1))#**

Usage

The "no" form of this command clears VRRP authentication.

Example

This example shows how to set the VRRP authentication password to "vrrpkey" on VLAN 1:

```
Matrix>Router(config)#interface vlan 1
Matrix>Router(config-if(Vlan 1))#ip vrrp authentication-key vrrpkey
```

ip vrrp message-digest-key

Use this command to set a VRRP MD5 authentication password on an interface.

Syntax

ip vrrp message-digest-key *vrid* **md5** *password* [**hmac-96**]

no ip vrrp message-digest-key

Parameters

vrid	Specifies the Virtual Router ID (VRID). Valid values are from **1** to **255**.
md5	Specifies the authentication type as MD5.
password	Specifies an MD5 authentication password. Text string can be 1 to 16 characters in length.
hmac-96	(Optional) If VRRP is running between Enterasys Matrix N or Enterasys Matrix E1 routers, this keyword is not required. If VRRP is run between an Enterasys Matrix N router and something other than an Enterasys Matrix E1 or an Enterasys Matrix N router, this keyword allows the md5 authentication to work between those routers.

Downloaded from www.Manualslib.com manuals search engine

Defaults

None.

Mode

Router command, Interface configuration: **Matrix>Router(config-if(Vlan 1))#**

Usage

The “no” form of this command clears VRRP MD5 authentication.

Example

This example shows how to set the VRRP MD5 authentication password to “qwer” on VLAN 1, VRID 1:

```
Matrix>Router(config)#interface vlan 1
Matrix>Router(config-if(Vlan 1))#ip vrrp message-digest-key 1 md5 qwer
```

show ip vrrp

Use this command to display VRRP routing information.

Syntax

show ip vrrp

Parameters

None.

Defaults

None.

Mode

Router command, Any router mode.

Example

This example shows how to display VRRP information:

```
Matrix>Router(config)#show ip vrrp

-----------VRRP CONFIGURATION-----------
Vlan   Vrid   State      Owner  AssocIpAddr      Priority  VirtMacAddr
256    1      Backup       0    172.3.56.20        100     0000.5e00.0101
                                 172.3.56.21
                                 172.3.56.22
```

Table 21-7 provides an explanation of the command output.

Downloaded from www.Manualslib.com manuals search engine

Table 21-7 show ip vrrp Output Details

Output...	What it displays...
Vlan	Specifies the VLAN on which this VRRP session resides.
Vrid	Specifies the Virtual Router ID associated with the routing interface.
State	Specifies the current state of the VRRP session as follows: **Stopped** - The Vrid is disabled. **Init** - The session is waiting in the init state. The vrid must be down due to the priority being set to zero, because one or more of the assigned critical ip interfaces has decremented the priority to 0. **Backup** - The Vrid is operating in the backup state. **Master** - The Vrid is operating in the master state. **ifDown** - The Vrid is down because the interface is not operational. **PreemptDel** - The Vrid is in a preempt delay state while transitioning to master.
Owner	Specifies whether this router owns the associated IP address as one of its interfaces. Valid values are: • **1** to indicate the router owns the address. • **0** to indicate the router does not own the address.
AssocIpAddr	Specifies the virtual IP address(es) associated with this VRRP session.
Priority	Specifies the priority value for this Vrid.
VirtMacAddr	Specifies the virtual MAC address for this VRRP session.

Downloaded from www.Manualslib.com manuals search engine

22

Port Priority and Rate Limiting Configuration

This chapter describes the Port Priority and Rate Limiting set of commands and how to use them.

For information about...	Refer to page...
Port Priority Configuration Summary	22-1
Configuring Port Priority	22-2
Configuring Priority to Transmit Queue Mapping	22-5
Configuring Port Traffic Rate Limiting	22-9

Port Priority Configuration Summary

The Enterasys Matrix Series device supports Class of Service (CoS), which allows you to assign mission-critical data to higher priority through the device by delaying less critical traffic during periods of congestion. The higher priority traffic through the device is serviced first before lower priority traffic. The Class of Service capability of the device is implemented by a priority queueing mechanism. Class of Service is based on the IEEE 802.1D (802.1p) standard specification, and allows you to define eight priorities (0 through 7) and, depending on port type, up to 16 transmit queues (0-15) of traffic for each port.

A priority 0 through 7 can be set on each port, with 0 being the lowest priority. A port receiving a frame without priority information in its tag header is assigned a priority according to the default priority setting on the port. For example, if the priority of a port is set to 4, the frames received through that port without a priority indicated in their tag header are classified as a priority 4 and transmitted according to that priority.

In addition, the device's rate limiting capabilities allow you to further prioritize traffic by limiting the rate of inbound or outbound traffic on a per port/priority basis.

Enterasys Networks' enhanced CoS implementation allows you to use the following methods to configure Class of Service on the Enterasys Matrix Series device:

- Configuring transmit queueing and rate limiting on a per-port basis as described in this chapter.
- Allowing the device to assign policy-based inbound rate limiters and transmit queues as described in Chapter 8.

Note: When CoS override is enabled using the **set policy profile** command as described in "set policy profile" on page 8-3, CoS-based classification rules will take precedence over priority settings configured with the **set port priority** command described in this section.

Downloaded from www.Manualslib.com manuals search engine

Configuring Port Priority

Purpose

To view or configure port priority characteristics as follows:

- Display or change the port default Class-of Service (CoS) transmit priority (0 through 7) of each port for frames that are received (ingress) without priority information in their tag header.
- Display the current traffic class mapping-to-priority of each port.
- Set each port to transmit frames according to 802.1D (802.1p) priority transmit queues set in the frame header.

Commands

For information about...	Refer to page...
show port priority	22-2
set port priority	22-3
clear port priority	22-3

show port priority

Use this command to display the 802.1D priority for one or more ports.

Syntax

show port priority [*port-string*]

Parameters

port-string	(Optional) Displays priority information for a specific port. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.

Defaults

If *port-string* is not specified, priority for all ports will be displayed.

Mode

Switch command, Read-Only.

Example

This example shows how to display the port priority for the fe.2.1 through 5:

```
Matrix(rw)->show port priority fe.2.1-5
fe.2.1 is set to 0
fe.2.2 is set to 0
fe.2.3 is set to 0
fe.2.4 is set to 0
```


Downloaded from www.Manualslib.com manuals search engine

```
fe.2.5 is set to 0
```

set port priority

Use this command to set the 802.1D (802.1p) Class-of-Service transmit queue priority (0 through 7) on each port.

Syntax

set port priority *port-string priority*

Parameters

port-string	Specifies the port for which to set priority. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.
priority	Specifies a value of **0** - **7** to set the CoS port priority for the port entered in the *port-string*. Port priority value of 0 is the lowest priority.

Defaults

None.

Mode

Switch command, Read-Write.

Usage

For information on how to configure protocol-based policy classification to a Class-of-Service, including how to configure a CoS policy to override port transmit queue priority, refer to Chapter 8.

When CoS override is enabled using the **set policy profile** command as described in "set policy profile" on page 8-3, CoS-based classification rules will take precedence over priority settings configured with this command.

A port receiving a frame without priority information in its tag header is assigned a priority according to the priority setting on the port. For example, if the priority of a port is set to 5, the frames received through that port without a priority indicated in their tag header are classified as a priority 5. A frame with priority information in its tag header is transmitted according to that priority.

Example

This example shows how to set a default priority of 6 on fe.1.3. Frames received by this port without priority information in their frame header are set to the default setting of 6:

```
Matrix(rw)->set port priority fe.1.3 6
```

clear port priority

Use this command to reset the current CoS port priority setting to 0.

Syntax

clear port priority *port-string*

Downloaded from www.Manualslib.com manuals search engine

Parameters

port-string	Specifies the port for which to clear priority. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.

Defaults

None.

Mode

Switch command, Read-Write.

Usage

This command will cause all frames received without a priority value in its header to be set to priority 0.

Example

This example shows how to reset fe.1.11 to the default priority:

```
Matrix(rw)->clear port priority fe.1.11
```


Downloaded from www.Manualslib.com manuals search engine

Configuring Priority to Transmit Queue Mapping

Purpose

To perform the following:

- View the current priority to transmit queue mapping of each port, which includes both physical and virtual ports.
- Configure each port to either transmit frames according to the port priority transmit queues (set using the **set port priority** command described back in "set port priority" on page 22-3), or according to a priority based on a percentage of port transmission capacity (set using the **set priority queue** command described in "set port priority-queue" on page 22-6).
- Clear current port priority queue settings for one or more ports.

Commands

For information about...	Refer to page...
show port priority-queue	22-5
set port priority-queue	22-6
clear port priority-queue	22-7

show port priority-queue

Use this command to display the port priority levels (0 through 7, with 0 as the lowest level) associated with the current transmit queue (0 - 15 depending on port type, with 0 being the lowest priority) for each priority of the selected port.

Syntax

show port priority-queue [*priority*]

Parameters

priority	(Optional) Displays queue levels for a specific priority value.

Defaults

If *priority* is not specified, all priority queue information will be displayed.

Mode

Switch command, Read-Only.

Usage

A frame with a certain port priority is transmitted according to the settings entered using the **set priority queue** command described in "set port priority-queue" on page 22-6.

Downloaded from www.Manualslib.com manuals search engine

Examples

This example shows how to display priority queue information for fe.1.7. In this case, the frames shown with a priority of 0 or 3 are transmitted according to the transmit priority queue of 1 (the second lowest transmit priority); frames with 1 or 2 priority, at the lowest transmit priority of 0; frames with 4 or 5 priority, at the second highest transmit priority of 2; and frames with 6 or 7 priority, at the highest transmit priority of 3:

```
Matrix(rw)->show port priority-queue fe.1.7
fe.1.7      Priority  TxQueue
----------  --------  -------
               0         1
               1         0
               2         0
               3         1
               4         2
               5         2
               6         3
               7         3
```

This example shows how to display the transmit queues associated with priority 3.

```
Matrix(rw)->show port priority-queue 3
fe.1.7     Priority  TxQueue
----------  --------  -------
               3         1
fe.1.8     Priority  TxQueue
----------  --------  -------
               3         1
fe.1.9     Priority  TxQueue
----------  --------  -------
               3         1
```

set port priority-queue

Use this command to map 802.1D (802.1p) priorities to transmit queues.

Syntax

set port priority-queue *port-string priority queue*

Downloaded from www.Manualslib.com manuals search engine

Parameters

port-string	Specifies the port(s) for which to set priority queue. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.
priority	Specifies a value of **0** - **7**(0 is the lowest level) that determines what priority frames will be transmitted at the priority queue level entered in this command.
queue	Specifies a value (0 is the lowest level) that determines when to transmit the frames with the port priority entered in this command. Number of transmit queues varies by port type. Typical values are: • 100Base-T - **4** • 1000Base-T - **4** • 1000Base-X - **8**

Defaults

None.

Mode

Read-Write.

Usage

This command enables you to change the priority queue (0-7, depending on port type, with 0 being the lowest priority queue) for each port priority of the selected port. You can apply the new settings to one or more ports. For example, if the priority queue is set to 3 for those frames with a port priority 4, then those frames would be transmitted before any frames contained in traffic classes 2 through 0.

Example

This example shows how to set priority 5 frames received on fe.2.12 to transmit at the lowest priority queue of 0.

```
Matrix(rw)->set port priority-queue fe.2.12 5 0
```

clear port priority-queue

Use this command to reset port priority queue settings back to defaults for one or more ports.

Syntax

clear port priority-queue *port-string*

Parameters

port-string	Specifies the port for which to clear priority queue. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.

Defaults

None.

Downloaded from www.Manualslib.com manuals search engine

Mode

Switch command, Read-Write.

Example

This example shows how to clear the priority queue settings on fe.2.12:

```
Matrix(rw)->clear port priority-queue fe.2.12
```

Usage

The total percentage of transmit queue values must add up to 100%.

Downloaded from www.Manualslib.com manuals search engine

Configuring Port Traffic Rate Limiting

Purpose

To limit the rate of inbound traffic on the Enterasys Matrix Series device on a per port/priority basis. The allowable range for the rate limiting is 125 kilobytes per second minimum up to the maximum transmission rate allowable on the interface type.

Rate limit is configured for a given port and list of priorities. The list of priorities can include one, some, or all of the eight 802.1p priority levels. Once configured, the rate of all traffic entering or leaving the port with the priorities configured to that port is not allowed to exceed the programmed limit. If the rate exceeds the programmed limit, frames are dropped until the rate falls below the limit.

Commands

For information about...	Refer to page...
show port ratelimit	22-9
set port ratelimit	22-10
clear port ratelimit	22-11

show port ratelimit

Use this command to show the traffic rate limiting configuration on one or more ports.

Syntax

show port ratelimit [*port-string*]

Parameters

port-string	(Optional) Displays rate limiting information for specific port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.

Defaults

If *port-string* is not specified, rate limiting information will be displayed for all ports.

Mode

Switch command, Read-Only.

Example

This example shows how to display the current rate limiting information for fe.2.1:

```
Matrix(rw)->show port ratelimit fe.2.1
Global Ratelimiting status is disabled.

    Port            Threshold                              Priority
   Number    Index   (kB/s)       Action     Direction      List      Status
```


Downloaded from www.Manualslib.com manuals search engine

```
-----------  -----  ---------  ------------  ---------  -----------  --------
fe.2.1           1     64125          discard    inbound            0     disabled
fe.2.1           2     64125          discard    inbound            0     disabled
fe.2.1           3     64125          discard    inbound            0     disabled
fe.2.1           4     64125          discard    inbound            0     disabled
fe.2.1           5     64125          discard    inbound            0     disabled
fe.2.1           6     64125          discard    inbound            0     disabled
fe.2.1           7     64125          discard    inbound            0     disabled
fe.2.1           8     64125          discard    inbound            0     disabled
fe.2.1           9     64125          discard    inbound            0     disabled
fe.2.1          10     64125          discard    inbound            0     disabled
fe.2.1          11     64125          discard    inbound            0     disabled
fe.2.1          12     64125          discard    inbound            0     disabled
```

Table 22-1 shows a detailed explanation of the command output.

Table 22-1 show port ratelimit Output Details

Output...	What it displays...
Port Number	Port designation. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.
Index	Resource index for this port.
Threshold (kB/s)	Port rate limiting threshold in kilobytes per second.
Action	Whether or not frames not conforming to rate limiting will be discarded.
Direction	This rule applies to inbound traffic.
Priority List	802.1D (802.1p) port priority level.
Status	Whether or not this rule is active or disabled.

set port ratelimit

Use this command to configure the traffic rate limiting status and threshold (in kilobytes per second) for one or more ports.

Syntax

set port ratelimit {**disable** | **enable**} | *port-string priority threshold* {**disable** | **enable**} [**inbound**] [*index*]

Parameters

disable | **enable**	When entered without a *port-string*, globally disables or enables the port rate limiting function. When entered with a *port-string*, disables or enables rate limiting on specific port(s) when the global function is enabled.
port-string	Specifies a port on which to set the rate limiting threshold and other parameters. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.

Downloaded from www.Manualslib.com manuals search engine

priority	Specifies the 802.1D (802.1p) port priority level associated with the *port-string*. Options are: • **0 - 7**, with 0 specifying the lowest priority, and • **all** to set the rate limiting threshold and other parameters on all port priority levels associated with the *port-string*.
threshold	Specifies a port rate limiting threshold in kilobytes per second. Range is **64** up to the maximum bytes per second rate for a given interface.
inbound	(Optional) Applies this rate policing rule to inbound or outbound traffic.
index	(Optional) Assigns a resource index for this port.

Defaults

- If not specified, threshold will be applied to inbound traffic on the port/priority.
- If *index* is not specified, settings will be applied to index 1, and will overwrite index 1 for any subsequent rate limits configured.

Mode

Switch command, Read-Write.

Example

This example shows how to:

- globally enable rate limiting
- configure rate limiting for inbound traffic on port fe.2.1, index 1, priority 5, to a threshold of 125 KBps:

```
Matrix(rw)->set port ratelimit enable
Matrix(rw)->set port ratelimit fe.2.1 5 125 enable inbound
```

clear port ratelimit

Use this command to clear rate limiting parameters for one or more ports.

Syntax

clear port ratelimit *port-string* [*index*]

Parameters

port-string	Specifies the port(s) on which to clear rate limiting. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.
index	(Optional) Specifies the associated resource index to be reset.

Defaults

If not specified, all *index* entries will be reset.

Mode

Switch command, Read-Write.

Downloaded from www.Manualslib.com manuals search engine

Example

This example shows how to clear all rate limiting parameters on port fe.2.:

```
1Matrix(rw)->clear port ratelimit fe.2.1
```


Downloaded from www.Manualslib.com manuals search engine

23

Transparent Web Cache Balancing Configuration

This chapter describes the Transparent Web Cache Balancing (TWCB) commands and how to use them.

Router: Unless otherwise specified, the commands covered in this chapter can be executed only when the device is in router mode. For details on how to enable router configuration modes, refer to *Enabling Router Configuration Modes* on page 2-103.

Note: An Enterasys Feature Guide document that contains a complete discussion on TWCB configuration exists at the following Enterasys web site: http://www.enterasys.com/support/manuals/

Understanding Transparent Web Cache Balancing (TWCB)

Transparent Web Cache Balancing (TWCB) provides for the storing of frequently accessed web objects on a cache of local servers. Each HTTP request is transparently redirected by the N-Series router to a configured cache server. When a user first accesses a web object that object is stored on a cache server. Each subsequent request for the object uses this cached object. Web caching allows multiple users to access web objects stored on local cache servers with a much faster response time than accessing the same objects over an internet connection or through a default gateway. This can also result in substantial cost savings by reducing the internet bandwidth usage.

The N-Series router does not act as a cache for web objects; rather, it redirects HTTP requests to local servers on which web objects are cached. The cache servers should have a web-based proxy cache running. The Squid application is an example of a web-based proxy cache.

Implementing a TWCB configuration requires users to configure a routed network with IP interfaces that allow the N-Series router to send requests for the internet to the correct web caching device.

There are five aspects to TWCB configuration:

- Create the server farms that will cache the web objects. A server farm is made up of 1 or more cache servers.
- Specify the end users whose HTTP requests will or will not be redirected to the cache servers. This step is optional. If no hosts are configured, the firmware redirects all HTTP requests.
- Specify the web site hosts that will not take part in TWCB.
- Create a web-cache that the server farms will be associated with.
- Apply the caching policy to an outbound interface to redirect HTTP traffic on that interface to the cache servers.

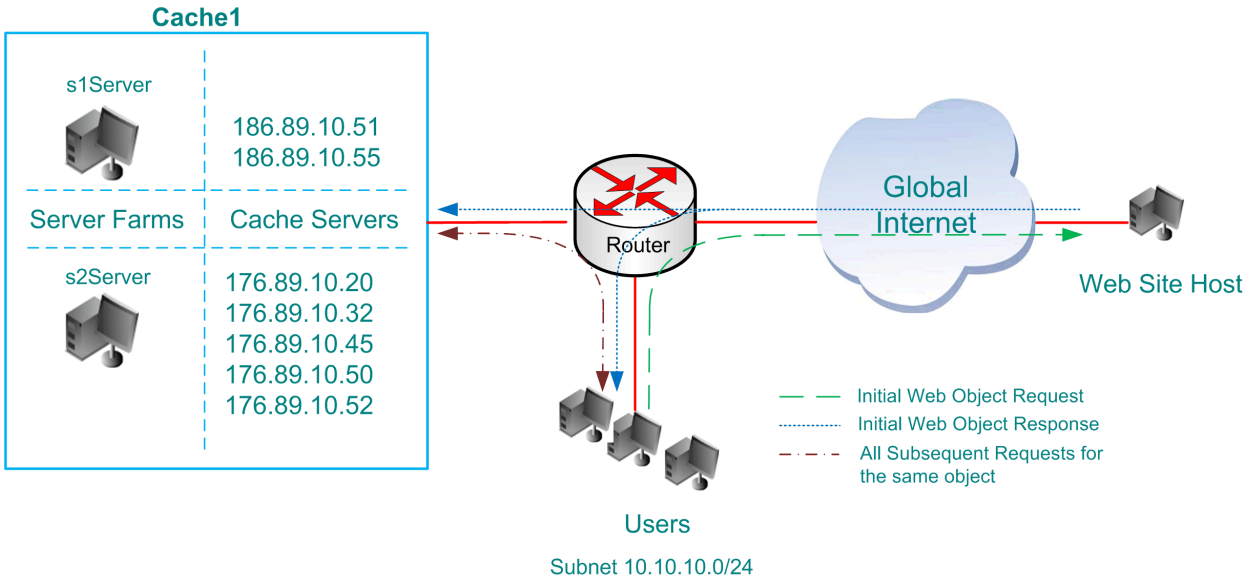
Figure 23-1 provides an example of a TWCB configuration overview. The web-cache is made up of server farms which logically group one or more cache servers. In our example, Cache1 is the name of the web-cache. It is made up of two server farms: s2Servers and s1Servers. The s1Server server

Downloaded from www.Manualslib.com manuals search engine

farm is configured with 2 cache servers from the 186.89.0.0 subnet. The s2Server server farm is configured with 5 cache servers from the 176.89.0.0 subnet.

A user on the 10.10.10.0/24 subnet makes a web request from the web site host. The response is sent to both the requesting user and a Cache1 cache server. The router determines the cache server on which an end-user's cache resides. Any future requests for that web object will be handled by the cache server until the cache entry expires. Cache entry expiration is configured in the web-based proxy cache application.

Figure 23-1 TWCB Configuration Overview



Purpose

To enable, configure and display information for Transparent Web Cache Balancing (TWCB) used to store frequently accessed web objects on a cache of local servers.

Commands

For information about...	Refer to page...
ip twcb wcserverfarm	23-3
predictor roundrobin	23-4
faildetect type	23-5
faildetect type	23-5
faildetect	23-6
maxconns	23-7
inservice	23-7
ip twcb webcache	23-8
http-port	23-9
serverfarm	23-9

Downloaded from www.Manualslib.com manuals search engine

For information about... (continued)	Refer to page...
bypass-list range	23-10
hosts redirect range	23-10
ip twcb redirect out	23-11
show ip twcb wcserverfarm	23-12
show ip twcb webcache	23-13
show ip twcb conns	23-13
show ip twcb stats	23-14
clear ip twcb statistics	23-14
show limits	23-15
set router limits (TWCB)	23-15
show router limits (TWCB)	23-16
clear router limits (TWCB)	23-17

ip twcb wcserverfarm

Use this command to create a web-cache server farm.

Syntax

ip twcb wcserverfarm *serverfarm-name*

Parameters

serverfarm-name	Specifies a server farm name. A maximum of 5 web-cache server farms are supported.

Defaults

None.

Mode

Router Configuration: **Matrix(rw)->Router(config)#**.

Usage

Executing this command enters server farm configuration command mode.

Example

This example creates the **s1Server** web-cache server farm:

```
Matrix(rw)->Router(config)#ip twcb wcserverfarm s1Server
Matrix(rw)->Router(config-twcb-wcsfarm)#
```


Downloaded from www.Manualslib.com manuals search engine

predictor roundrobin

Use this command to modify the round-robin predictor value by applying a list of destination IP addresses for which the cache servers within this server farm will be selected by the round-robin algorithm.

Syntax

predictor roundrobin *ip-address-begin ip-address-end*

Parameters

ip-address-begin	The beginning IP address of a list of destination IP addresses for which the cache servers within this server farm will be selected by the round-robin algorithm.
ip-address-end	The ending IP address of a list of destination IP addresses for which the cache servers within this server farm will be selected by the round-robin algorithm.

Defaults

None.

Mode

Router command, Server Farm Configuration mode: **Matrix(rw)->Router(config-twcb-wcsfarm)#**.

Usage

The router uses the end-user IP address, making the HTTP request, to determine which cache server it will send the request to. If a web site is accessed frequently, the cache server serving requests for this end-user ip address may become overloaded with user requests. You can specify end-user ip addresses be distributed across the cache servers of this server farm in a round-robin algorithm using the predictor roundrobin command.

When a predictor round-robin user list is configured, only users in configured lists are cached in cache servers belonging to this server farm. If no predictor round-robin user list is configured for a server farm, all other users not configured in a predictor round-robin user list on some other server farm may be cached in the cache servers belonging to this server farm.

Up to 10 separate lists can be defined per server farm. The destination IP addresses specified can not be already configured within any other round-robin destination IP list.

Example

This example configures a predictor round-robin for the web-cache server farm **s1Server** specifying that the end users with IP addresses from **10.10.10.05** through **10.10.10.25** should be selected on a round-robin basis for caching on cache servers belonging to this server farm:

```
Matrix(rw)->Router(config)#ip twcb wcserverfarm s1Server
Matrix(rw)->Router(config-twcb-wcsfarm)#predictor roundrobin 10.10.10.05
10.10.10.25
```


Downloaded from www.Manualslib.com manuals search engine

cache

Use this command to create a cache server based upon the supplied IP address.

Syntax

cache *ip-address*

Parameters

ip-address	Specifies the IP address of the cache server to be created.

Defaults

None.

Mode

Router command, Server Farm Configuration mode: **Matrix(rw)->Router(config-twcb-wcsfarm)#**.

Usage

The firmware supports 128 cache servers.

Executing this command enters cache server configuration command mode.

Example

This example configures IP address **186.89.10.51** as a cache server on the **s1Server** server farm:

```
Matrix(rw)->Router(config)#ip twcb wcserverfarm s1Server
Matrix(rw)->Router(config-twcb-wcsfarm)#cache 186.89.10.51
Matrix(rw)->Router(config-twcb-cache)#
```

faildetect type

Use this command to specify the TWCB cache server up or down status detection method.

Syntax

faildetect type [**ping** | **app** | **both**]

Parameters

ping	(Optional) Specifies the ping method for detection of TWCB cache server up or down status.
app	(Optional) Specifies the application method for detection of TWCB cache server up or down status.
both	(Optional) Specifies that both ping and app detection types should be used for the detection of TWCB cache server up or down status.

Defaults

If no parameter is specified, the Ping method is used.

Downloaded from www.Manualslib.com manuals search engine

Mode

Router command, Cache Server Configuration mode: **Matrix(rw)->Router(config-twcb-cache)#**.

Usage

The application method defaults to a check of service availability on port 80. This check can be overridden by the web-cache group configuration of **http-port** using the http-port command.

Example

This example sets the failure detection type to the **ping** method for cache server **186.89.10.51**:

```
Matrix(rw)->Router(config)#ip twcb wcserverfarm s1Server
Matrix(rw)->Router(config-twcb-wcsfarm)#cache 186.89.10.51
Matrix(rw)->Router(config-twcb-cache)#faildetect type ping
```

faildetect

Use this command to specify the TWCB cache server up or down status detection method parameter values.

Syntax

faildetect [**ping-int** *seconds*] [**ping-retries** *number*] [**app-int** *seconds* **app-retries** *number*]

Parameters

ping-int *seconds*	(Optional) Specifies the interval between pings in seconds. Values range from 1 to 3600. Default value of 5.
ping-retries *number*	(Optional) Specifies the number of ping retries in seconds before declaring the cache server down. Values range from 1 to 255. Default value of 4.
app-int *seconds*	(Optional) Specifies the interval between app retries in seconds. Values range from 1 - 3600. Default value of 15.
app-retries *number*	(Optional) Specifies the number of retries before declaring the cache server down. Values range of 1 to 255. Default value of 4.

Defaults

If no parameter is specified, all parameters remain unchanged.

Mode

Router command, Cache Server Configuration mode: **Matrix(rw)->Router(config-twcb-cache)#**.

Example

This example sets the failure detection type to the **ping** method for cache server **186.89.10.51** and sets the ping interval to **7** and the number of ping retries to **3**:

```
Matrix(rw)->Router(config)#ip twcb wcserverfarm s1Server
Matrix(rw)->Router(config-twcb-wcsfarm)#cache 186.89.10.51
Matrix(rw)->Router(config-twcb-cache)#faildetect type ping
Matrix(rw)->Router(config-twcb-cache)#faildetect ping-int 7 ping-retries 3
```


Downloaded from www.Manualslib.com manuals search engine

maxconns

Use this command to limit the maximum number of connections to the server.

Syntax

maxconns *number*

Parameters

number	Specifies the maximum number of connections allowed for this server. Values range from 1 to 5000. Default value of 5000.

Defaults

None.

Mode

Router command, Cache Server Configuration mode: **Matrix(rw)->Router(config-twcb-cache)#**.

Example

This example sets the maximum number of connections for cache server **186.89.10.51** to **1000**:

```
Matrix(rw)->Router(config)#ip twcb wcserverfarm s1Server
Matrix(rw)->Router(config-twcb-wcsfarm)#cache 186.89.10.51
Matrix(rw)->Router(config-twcb-cache)#maxconns 1000
```

inservice

Use this command to activate this cache server or web-cache.

Syntax

inservice

Parameters

None.

Defaults

None.

Mode

Router command, Cache Server Configuration: **Matrix(rw)->Router(config-twcb-cache)#** or Web-Cache Configuration mode: **Matrix(rw)->Router(config-twcb-webcache)#**.

Usage

Enter the inservice command after all other parameters are configured for the cache server or web-cache context.

At least one cache server must be in service in order to place a web-cache in service.

Downloaded from www.Manualslib.com manuals search engine

Examples

This example sets the maximum number of connections for cache server **186.89.10.51** to **100** and activates the server:

```
Matrix(rw)->Router(config)#ip twcb wcserverfarm s1Server
Matrix(rw)->Router(config-twcb-wcsfarm)#cache 186.89.10.51
Matrix(rw)->Router(config-twcb-cache)#maxconns 100
Matrix(rw)->Router(config-twcb-cache)#inservice
```

This example adds the web-cache server farm **s1Server** to the **cache1** web-cache and activates the web-cache:

```
Matrix(rw)->Router(config)#ip twcb webcache cache1
Matrix(rw)->Router(config-twcb-webcache)#serverfarm s1Server
Matrix(rw)->Router(config-twcb-webcache)#inservice
```

ip twcb webcache

Use this command to create a web-cache using the specified name.

Syntax

ip twcb webcache *web-cache-name*

Parameters

web-cache-name	Specifies the name of the web-cache to be created. Firmware supports the creation of 1 web-cache.

Defaults

None.

Mode

Router Configuration mode: **Matrix(rw)->Router(config)#**.

Usage

Before a web-cache can be put in service there must be at least one cache server associated with it that is in service.

Executing this command enters web-cache comfiguration command mode.

Example

This example creates a web-cache named **cache1**:

```
Matrix(rw)->Router(config)#ip twcb webcache cache1
Matrix(rw)->Router(config-twcb-webcache)#
```


Downloaded from www.Manualslib.com manuals search engine

http-port

Use this command to redirect outbound HTTP requests to a non-standard HTTP port number.

Syntax

http-port *port-number*

Parameters

port-number	Specifies the non-standard HTTP port number to redirect outbound HTTP requests to. Default value of 80.

Defaults

None.

Mode

Router command, web-cache Configuration mode: **Matrix(rw)->Router(config-twcb-webcache)#**.

Example

This example changes the HTTP port for web-cache **cache1** to **8080**:

```
Matrix(rw)->Router(config)#ip twcb webcache cache1
Matrix(rw)->Router(config-twcb-webcache)#http-port 8080
```

serverfarm

Use this command to add the specified server farm to this web-cache.

Syntax

serverfarm *serverfarm-name*

Parameters

serverfarm-name	Specifies the name of the server farm to add to this web-cache.

Defaults

None.

Mode

Router command, Cache Server Configuration mode: **Matrix(rw)->Router(config-twcb-webcache)#**.

Usage

The firmware supports a maximum of 5 server farms.

Downloaded from www.Manualslib.com manuals search engine

Example

This example adds the server farm **s1Server** to the **cache1** web-cache:

```
Matrix(rw)->Router(config)#ip twcb webcache cache1
Matrix(rw)->Router(config-twcb-webcache)#serverfarm s1Server
```

bypass-list range

Use this command to specify web host sites for which HTTP requests are not redirected to the cache servers.

Syntax

bypass-list range *begin-ip-address end-ip-address*

Parameters

begin-ip-address	Specifes an IP address that begins a range of IP addresses of sites for which HTTP requests are not redirected to the cache servers.
end-ip-address	Specifies an IP address that ends a range of IP addresses of sites for which HTTP requiests are not redirected to the cache servers.

Defaults

None.

Mode

Router command, Cache Server Configuration mode: **Matrix(rw)->Router(config-twcb-webcache)#**.

Usage

Some web site hosts require source IP address authentication for user access. HTTP requests for these sites can not be redirected to the cache servers. This command provides for the creation of lists of IP addresses that need to bypass the cache servers.

Example

This example creates a bypass list for web-cache **cache1** for IP address range **50.10.10.30** to **50.10.10.43**:

```
Matrix(rw)->Router(config)#ip twcb webcache cache1
Matrix(rw)->Router(config-twcb-webcache)#bypass-list range 50.10.10.30
50.10.10.43
```

hosts redirect range

Use this command to explicitly permit or deny redirection of HTTP requests for the list of end users to this web-cache.

Syntax

hosts {**permit** | **deny**} **redirect range** *begin-ip-address end-ip-address*

Downloaded from www.Manualslib.com manuals search engine

Parameters

begin-ip-address	Specifies an IP address that begins a range to explicitly permit or deny redirection of HTTP requests from these end users to this web-cache.
end-ip-address	Specifies an IP address that ends a range to explicitly permit or deny redirection of HTTP requests from these end users to this web-cache.

Defaults

None.

Mode

Router command, Cache Server Configuration mode: **Matrix(rw)->Router(config-twcb-webcache)#**.

Usage

You can explicitly specify end user clients whose HTTP requests are or are not redirected to the cache servers. If you do not explicitly specify such addresses, HTTP requests from all end users are redirected to the cache server.

Example

This example configures a **deny** list for end users **10.10.10.26** through **10.10.10.50** to have HTTP requests redirected to this web-cache:

```
Matrix(rw)->Router(config)#ip twcb webcache cache1
Matrix(rw)->Router(config-twcb-webcache)#hosts deny redirect range 10.10.10.26
10.10.10.50
```

ip twcb redirect out

Use this command to redirect outbound HTTP traffic from an interface to the cache servers.

Syntax

ip twcb *webcache-name* **redirect out**

Parameters

webcache-name	Specifies the name of the web-cache to redirect outbound HTTP traffic to.

Defaults

None.

Mode

Router command, Interface Configuration mode: **Matrix>Router(config-if(Vlan 1))#**.

Usage

The outbound interface is typically an interface that connects to the Internet. Associate the specified web-cache to the indicated VLAN for redirection of HTTP traffic. Up to 3 interfaces can be associated with a web-cache.

Downloaded from www.Manualslib.com manuals search engine

Example

This example associates the **cache1** web-cache with **vlan 1** for the redirection of HTTP traffic:

```
Matrix(rw)->router
Matrix>router>enable
Matrix>router#configure terminal
Enter configuration commands:
Matrix>Router(config)#interface vlan 1
Matrix>Router(config-if(Vlan 1))#ip twcb cache1 redirect out
```

show ip twcb wcserverfarm

Use this command to display configuration data for the specified server farm.

Syntax

show ip twcb wcserverfarm [*serverfarm-name*]

Parameters

serverfarm-name	(Optional) Specifies the server farm for the display of configuration data.

Defaults

If no parameter is specified, displays details for all configured server farms.

Mode

Router command: **Matrix(rw)->Router#**.

Examples

This example displays configuration data for the **s1Server** server farm:

```
Matrix(rw)->Router#show ip twcb wcserverfarm s1Server
Server Farm                    Configured      Active
  Name:        Predictor       Cache Servers   Cache Servers
-------------------------------------------------------------
s1Server        ROUNDROBIN        3               2
```

This example displays configuration data for all of the server farms for this web-cache:

```
Matrix>Router#show ip twcb wcserverfarm
Server Farm                    Configured      Active
  Name:        Predictor       Cache Servers   Cache Servers
-------------------------------------------------------------
s1Server       ROUNDROBIN         3              2
s2Server       ROUNDROBIN         2              2
s3Server       HASH               4              2
```


Downloaded from www.Manualslib.com manuals search engine

show ip twcb webcache

Use this command to display configuration data associated with the specified web-cache.

Syntax

show ip twcb webcache [*webcache-name*]

Parameters

webcache-name	(Optional) Specifies the name of the web-cache for the display of configuration data.

Defaults

If no parameter is specified, information for all web-caches is displayed.

Mode

Router command: **Matrix(rw)->Router#**.

Example

This example displays configuration data for the **cache1** web-cache:

```
Matrix(rw)->Router#show ip twcb webcache
Web Cache      Applied           Http      Active        Active
Name:          Interface         Port      Status        Server Farms
-------------------------------------------------------------------------
cache1         Vlan1             80        inservice     s1Server
                                                         s2Server
```

show ip twcb conns

Use this command to display cache server connection data.

Syntax

show ip twcb conns [**client** *ip-address* | **wcserver** *webcache-name*]

Parameters

client *ip-address*	(Optional) Specifies a particular client for the display of connection data.
wcserver *webcache-name*	(Optional) Specifies a particular web-cache for the display of connection data.

Defaults

If no parameter is specified, connection data for all clients and cache servers is displayed.

Mode

Router Command: **Matrix(rw)->Router#**.

Downloaded from www.Manualslib.com manuals search engine

Example

This example displays connection data for the all cache servers and all clients:

```
Matrix(rw)->Router#show ip twcb conns
flo-id   cache-server-ip   client-ip       cport  state
-----------------------------------------------------------------
1        172.17.1.2        169.254.1.52    80     OUT-SERVR REPLY
```

show ip twcb stats

Use this command to display cache server connection stats data.

Syntax

show ip twcb stats

Parameters

None.

Defaults

None.

Mode

Router Command: **Matrix(rw)->Router#**.

Example

This example displays connection stats data for all clients and cache servers:

```
Matrix(rw)->Router#show ip twcb stats
created         established     deleted         No Available
connections     connections     connections     Binding Resources
-------------------------------------------------------------------------------
   4                1               3                0
```

clear ip twcb statistics

Use this command to reset the statistical data for the specified web-cache.

Syntax

clear ip twcb statistics [*webcache-name*] [**all**]

Parameters

webcache-name	(Optional) Specifies the web-cache to clear statistics on.
all	(Optional) Specifies that statistics should be cleared on all web-caches, server farms and cache servers. This is the default for this command.

Downloaded from www.Manualslib.com manuals search engine

Defaults

If no parameter is specified, statistics for all web-caches, server farms, and cache servers are cleared.

Mode

Router Command: **Matrix(rw)->Router#**.

Example

This example clears statistics for all web-caches, web-cache server farms and cache servers:

```
Matrix(rw)->Router#clear ip twcb statistics
```

show limits

Use this command to display the TWCB entry and memory limits.

Syntax

show limits

Parameters

None.

Defaults

None.

Mode

Router Command: **Matrix(rw)->Router#**.

Example

This example displays the TWCB entry and memory limit statistics:

```
Matrix(rw)->Router#show limits
                                |          Entries         |        Memory (bytes)
 (256 MgB)       Resource       |   Max-  InUse=    Avail  | Each ~=  Max        InUse
                 ========       |   ===== =====     =====  | ===== =======       =====

   TWCB Webcache Server Cfg     |      50     0        50  | 19688  984400         0
          TWCB Cache Binding    |    5000     0      5000  |   216 1080000         0
```

set router limits (TWCB)

Use this command to set TWCB bindings, cache, and configuration limits.

Syntax

set router limits {**twcb-bindings** *twcb-bindings* | **twcb-cache** *twcb-cache* | **twcb-configs** *twcb-configs*}

Downloaded from www.Manualslib.com manuals search engine

Parameters

twcb-bindings *twcb-bindings*	(Optional) Specifies the maximum number of TWCB bindings for this router. Values range from 1000 to 32000. Default value of 32000.
twcb-cache *twcb-cache*	(Optional) Specifies the maximum TWCB cache size for this router. Values range from 500 to 10000. Default value of 2000.
twcb-configs *twcb-configs*	(Optional) Specifies the maximum number of web-cache configurations. Maximum and Default value of 1.

Defaults

None.

Mode

Switch Command: **Matrix(rw)->**.

Usage

Bindings and cache use valuable memory resources and are shared on a first come first serve basis across a number of applications. Use this command to free memory resources to be user by other applications by limiting the number of TWCB bindings and cache size allowed.

Currently, only a single web-cache is supported. The TWCB configs setting exists for future use.

The chassis or system must be rebooted for any new change to take effect.

This command must be executed from the switch CLI.



Note: Router limits can also be set in the following contexts:

To set LSNAT router limits see *set router limits (LSNAT)* on page 19-33.

To set NAT router limits see *set router limits (NAT)* on page 18-14.

Example

This example sets the maximum TWCB cache size to 5000:

```
Matrix(rw)-> set router limits twcb-cache 5000
```

show router limits (TWCB)

Use this command to display TWCB router limit configuration settings.

Syntax

show router limits [**twcb-bindings**] [**twcb-cache**] [**twcb-configs**]

Parameters

twcb-bindings	(Optional) Displays the TWCB maximum bindings limit.
twcb-cache	(Optional) Displays the TWCB cache size limit.
twcb-configs	(Optional) Displays the TWCB configuration limit.

Defaults

If no parameter is specified, all router limit settings are displayed.

Downloaded from www.Manualslib.com manuals search engine

Mode

Switch command mode: **Matrix(rw)->**.

Examples

This example displays all router limits for this system:

```
Matrix(su)->show router limits
LSNAT maximum Bindings                          -  32000  (default)
LSNAT Cache size                                -   2000  (default)
LSNAT maximum Configs                           -     50  (default)
NAT maximum Bindings                            -  32000  (default)
NAT Cache size                                  -   2000  (default)
NAT maximum dynamic mapping Configs             -     10  (default)
NAT maximum static mapping Configs              -     50  (default)
NAT maximum Interface Configs                   -    103  (default)
NAT maximum global address Configs              -   1000  (default)
NAT maximum global port Configs                 -  32000  (default)
Route Table Limit                               -  12000  (default)
TWCB maximum Bindings                           -  32000  (default)
TWCB Cache size                                 -   2000  (default)
TWCB maximum Configs                            -      1  (default)
```

This example displays the TWCB cache-size limit for this system:

```
Matrix(su)->show router limits twcb-cache
TWCB Cache size                                 -   2000  (default)
```

clear router limits (TWCB)

Use this command to reset TWCB router limits to the default values.

Syntax

clear router limits [**twcb-binding**] [**twcb-cache**] [**twcb-configs**]

Parameters

twcb-binding	(Optional) Specifies the resetting of TWCB binding router limits to the default value.
twcb-cache	(Optional) Specifies the resetting of TWCB cache size router limits to the default value.
twcb-configs	(Optional) Specifies the resetting the number of TWCB configurations to the default value.

Defaults

If no parameters are specified, all router limits are reset, including NAT and LSNAT router limits.

Mode

Switch Command: **Matrix(rw)->**.

Downloaded from www.Manualslib.com manuals search engine

Usage

This command must be executed from the switch CLI.



Note: Router limits can also be cleared in the following contexts:

To clear LSNAT router limits see *clear router limits (LSNAT)* on page 19-34.

To clear NAT router limits see *clear router limits (NAT)* on page 18-16.

If you do not specify a parameter when issueing a **clear router limits** command, router limits for TWCB, LSNAT, and NAT contexts are reset to the default value.

Example

This example resets the TWCB cache router limits setting to the default value:

```
Matrix(rw)->clear router limits twcb-cache
```


Downloaded from www.Manualslib.com manuals search engine

TWCB Configuration Example

In this TWCB configuration example we will step through the configuration of two server farms named s1Server and s2Server. The S1Server server farm will have round-robin predictor end-user ranges associated with it from both the 20.10.10.0/24 subnet and the 10.10.10.0/24 subnet, for users with an expectation of heavy web-site access requirements. All other users not members of a predictor round-robin list or denied host redirect will use the s2Server server farm with a standard cache.

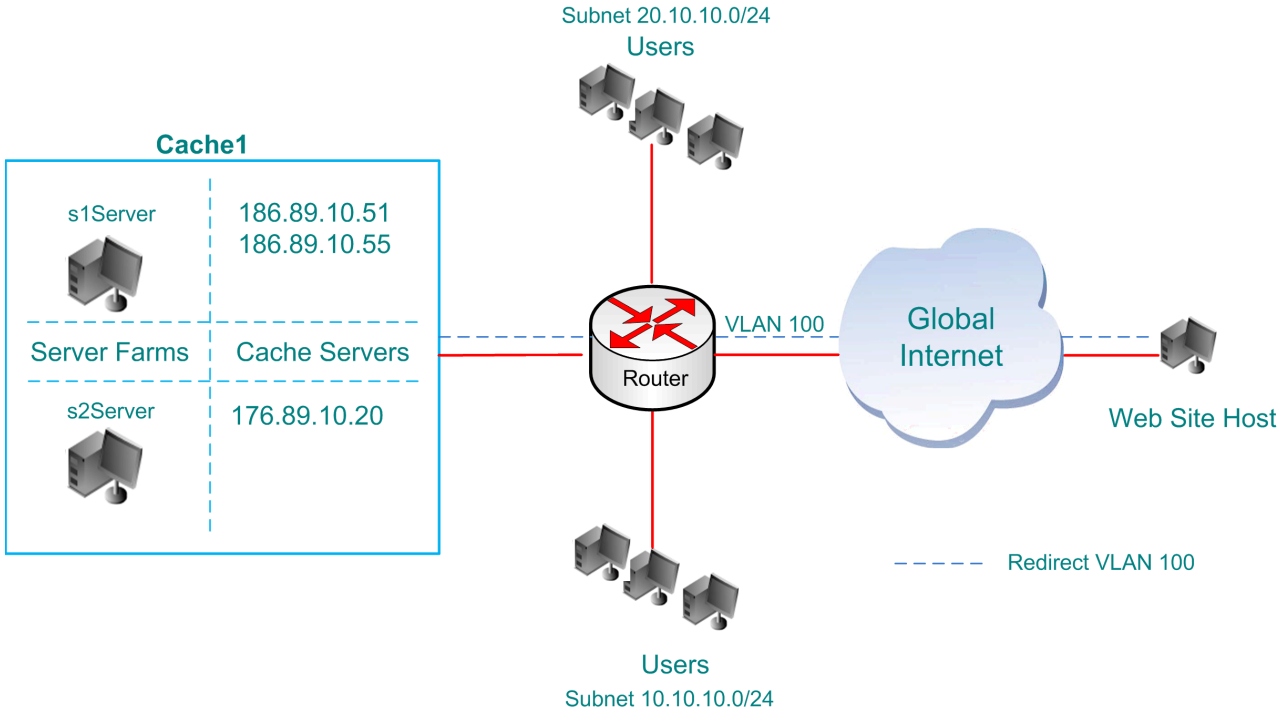
The s1Server will have cache servers 186.89.10.51 and 186.89.10.55 associated with it. The s2Server will have cache server 196.89.10.20 associated with it. s1Server cache servers will use faildetect type ping with faildetect parameter values changed to an interval of 4 seconds and the number of retries to 5. The s2Server cache servers will use the application faildetect type, with faildetect parameter values changed to an interval of 12 seconds and the number of retries to 5. The maximum number of connections per cache server will be configured for 800 for both server farms.

The web-cache will be configured as cache1. The HTTP port being used has been changed from the default of 80 to 8080. A bypass list has been configured to deny TWCB functionality for web requests to web host sites 50.10.10.30 to 50.10.10.43 because these sites require IP address authentication for user access. End-users 10.10.10.25 to 10.10.10.30 have been configured to deny TWCB functionality.

On the switch TWCB router bindings are limited to 20,000 and the TWCB cache size is limited to 5000.

See Figure 23-2 for a depiction of the example setup.

Figure 23-2 TWCB Configuration Example Overview



Configure the s1Server Server Farm

Create the server farm:

Downloaded from www.Manualslib.com manuals search engine

```
Matrix>router
Matrix>Router>enable
Matrix>Router>#configure
Enter configuration commands:
Matrix>Router(config)#ip twcb wcserverfarm s1Server
Matrix>Router(config-twcb-wcsfarm)#
```

Configure the end-users that will use this server farm by setting the round-robin predictor ranges:

```
Matrix>Router(config-twcb-wcsfarm)#predictor roundrobin 10.10.10.01 10.10.10.15
Matrix>Router(config-twcb-wcsfarm)#predictor roundrobin 20.10.10.25 10.10.10.60
Matrix>Router(config-twcb-wcsfarm)#
```

Configure cache server 186.89.10.51:

```
Matrix>Router(config-twcb-wcsfarm)#cache 186.89.10.51
Matrix>Router(config-twcb-cache)#faildetect type ping
Matrix>Router(config-twcb-cache)#faildetect ping-int 4
Matrix>Router(config-twcb-cache)#faildetect ping-retries 5
Matrix>Router(config-twcb-cache)#maxconns 800
Matrix>Router(config-twcb-cache)#inservice
Matrix>Router(config-twcb-cache)#exit
Matrix>Router(config-twcb-wcsfarm)#
```

Configure cache server 186.89.10.55:

```
Matrix>Router(config-twcb-wcsfarm)#cache 186.89.10.55
Matrix>Router(config-twcb-cache)#faildetect type ping
Matrix>Router(config-twcb-cache)#faildetect ping-int 4
Matrix>Router(config-twcb-cache)#faildetect ping-retries 5
Matrix>Router(config-twcb-cache)#maxconns 800
Matrix>Router(config-twcb-cache)#inservice
Matrix>Router(config-twcb-cache)#exit
Matrix>Router(config-twcb-wcsfarm)#exit
Matrix>Router(config)#
```

Configure the s2Server Server Farm

Configure server farm s2Server:

```
Matrix>Router(config)#ip twcb wcserverfarm s2Server
Matrix>Router(config-twcb-wcsfarm)#
```

Configure cache server 176.89.10.20:

```
Matrix>Router(config-twcb-wcsfarm)#cache 176.89.10.20
Matrix>Router(config-twcb-cache)#faildetect type app
Matrix>Router(config-twcb-cache)#faildetect app-int 12
Matrix>Router(config-twcb-cache)#faildetect app-retries 5
Matrix>Router(config-twcb-cache)#maxconns 800
Matrix>Router(config-twcb-cache)#inservice
Matrix>Router(config-twcb-cache)#exit
```


Downloaded from www.Manualslib.com manuals search engine

```
Matrix>Router(config-twcb-wcsfarm)#exit
Matrix>Router(config)#
```

Configure the cache1 Web Cache

Configure the web-cache cache1:

```
Matrix>Router(config)#ip twcb webcache cache1
Matrix>Router(config-twcb-webcache)#http-port 8080
Matrix>Router(config-twcb-webcache)#serverfarm s1Server
Matrix>Router(config-twcb-webcache)#serverfarm s2Server
Matrix>Router(config-twcb-webcache)#bypass-list range 50.10.10.30 50.10.10.43
Matrix>Router(config-twcb-webcache)#hosts redirect deny redirect range
10.10.10.25 10.10.10.30
Matrix>Router(config-twcb-webcache)#exit
Matrix>Router(config)#
```

Configure the outbound interface that connects with the internet:

```
Matrix>Router(config)#interface vlan 100
Matrix>Router(config-if(Vlan 1))#ip twcb cache1 redirect out
Matrix>Router(config-if(Vlan 1))#end
Matrix>Router#
```

Configure the Switch and Router

Configure the TWCB router limits:

```
Matrix(rw)-> set router limits twcb-bindings 20000
Matrix(rw)-> set router limits twcb-cache 5000
```

Clear the statistical data for this web-cache:

```
Matrix(rw)->Router#clear ip twcb statistics
```

This completes the TWCB configuration example.

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

24

Security Configuration

This chapter describes the Security Configuration set of commands and how to use them.

For information about...	Refer to page...
Overview of Security Methods	24-1
Configuring MAC Locking	24-2
Configuring Secure Shell (SSH)	24-11
Configuring Access Lists	24-15
Configuring Denial of Service (DoS) Prevention	24-22
Configuring Flow Setup Throttling (FST)	24-25

Overview of Security Methods

The following security methods are available for controlling which users are allowed to access, monitor, and manage the device.

- Local user credentials — used for local authentication and authorization of CLI and WebView management sessions. For details, refer to "Setting User Accounts and Passwords" on page 2-15 and "Setting the Authentication Login Method" on page 25-50.
- SNMP user or community names — used for authentication and authorization of all SNMP requests. For details, refer to Chapter 5.
- MAC Locking — locks a port to one or more MAC addresses, preventing connection of unauthorized devices via the port. For details, refer to "Configuring MAC Locking" on page 24-2.
- Secure Shell (SSH) — provides for secure remote CLI management access. For details, refer to "Configuring Secure Shell (SSH)" on page 24-11.
- IP Access Lists (ACLs) — permits or denies access to routing interfaces based on protocol and inbound and/or outbound IP address restrictions configured in access lists. For details, refer to "Configuring Access Lists" on page 24-15.
- Policy-Based Routing — permits or denies access to routing interfaces based on access lists in a route map applied to the interface. For details, refer to "Configuring Denial of Service (DoS) Prevention" on page 24-22.
- Denial of Service (DoS) Prevention — prevents Denial of Service attacks, including land, fragmented and large ICMP packets, spoofed address attacks, and UDP/TCP port scanning. For details, refer to "Configuring Denial of Service (DoS) Prevention" on page 24-22.

Downloaded from www.Manualslib.com manuals search engine

- Flow Setup Throttling (FST) — prevents the effects of DoS attacks by limiting the number of new or established flows that can be programmed on any individual switch port. For details, refer to "Configuring Flow Setup Throttling (FST)" on page 24-25.

Configuring MAC Locking

Purpose

To review, disable, enable and configure MAC locking. This locks a MAC address to one or more ports, preventing connection of unauthorized devices via the port(s). When source MAC addresses are received on specified ports, the switch discards all subsequent frames not containing the configured source addresses. The only frames forwarded on a "locked" port are those with the "locked" MAC address(es) for that port.



Note: Matrix DFE-Gold Series modules allow for up to 32 MAC addresses to be locked per port.

Commands

For information about...	Refer to page...
show maclock	24-2
show maclock stations	24-4
set maclock enable	24-5
set maclock disable	24-5
set maclock	24-6
set maclock firstarrival	24-7
set maclock move	24-7
clear maclock firstarrival	24-8
set maclock static	24-8
clear maclock static	24-9
set maclock trap	24-9
clear maclock	24-10

show maclock

Use this command to display the status of MAC locking on one or more ports.

Syntax

show maclock [*port_string*]

Downloaded from www.Manualslib.com manuals search engine

Parameters

port_string	(Optional) Displays MAC locking status for specified port(s). For a detailed description of possible *port_string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.

Defaults

If *port_string* is not specified, MAC locking status will be displayed for all ports.

Mode

Switch command, Read-Only.

Example

This example shows how to display MAC locking information for ge.2.1 through 5:

```
Matrix(rw)->show maclock ge.2.1-5

MAC locking is globally enabled.

  Port      Port     Trap     Max Static  Max FirstArrival      Violating
 Number    Status   Status    Allocated     Allocated          MAC Address
--------  --------  --------  ----------  ----------------  -----------------
ge.2.1    enabled   enabled   20          600               00-00-00-00-00-00
ge.2.2    enabled   enabled   20          600               00-00-00-00-00-00
ge.2.3    enabled   enabled   20          600               00-00-00-00-00-00
ge.2.4    enabled   enabled   20          600               00-00-00-00-00-00
ge.2.5    enabled   enabled   20          600               00-00-00-00-00-00
```

Table 24-1 provides an explanation of the command output.

Table 24-1 show maclock Output Details

Output...	What it displays...
Port Number	Port designation. For a detailed description of possible *port_string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.
Port Status	Whether MAC locking is **enabled** or **disabled** on the port. MAC locking is globally disabled by default. For details on using **set maclock** commands to enable it on the device and on one or more ports, refer to "set maclock enable" on page 24-5 and "set maclock" on page 24-6.
Trap Status	Whether MAC lock trap messaging is **enabled** or **disabled** on the port. For details on setting this status using the **set maclock trap** command, refer to "set maclock trap" on page 24-9.
Max Static Allocated	The maximum static MAC addresses allowed locked to the port. For details on setting this value using the **set maclock static** command, refer to "set maclock static" on page 24-8.
Max FirstArrival Allocated	The maximum end station MAC addresses allowed locked to the port. For details on setting this value using the **set maclock firstarrival** command, refer to "set maclock firstarrival" on page 24-7.
Violating MAC Address	Most recent MAC address(es) violating the maximum static and first arrival value(s) set for the port.

Downloaded from www.Manualslib.com manuals search engine

show maclock stations

Use this command to display MAC locking information about end stations connected to the device.

Syntax

show maclock stations [**firstarrival** | **static**] [*port-string*]

Parameters

firstarrival	(Optional) Displays MAC locking information about end stations first connected to MAC locked ports.
static	(Optional) Displays only MAC locking information about static (management defined) end stations connected to MAC locked ports.
port_string	(Optional) Displays end station information for specified port(s). For a detailed description of possible *port_string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.

Defaults

If no parameters are specified, MAC locking information will be displayed for end stations in the stations table. This does not include static configured end stations.

Mode

Switch command, Read-Only.

Example

This example shows how to display MAC locking information for the end stations connected to all Fast Ethernet ports in module 2:

```
Matrix(rw)->show maclock stations fe.2.*
Port Number   MAC Address         Status          State
------------  -----------------   --------------  --------------
fe.2.3        00-10-a4-e5-08-4e   active          first learned
fe.2.3        08-00-20-7c-e0-db   active          first learned
fe.2.6        00-60-08-14-4b-15   active          first learned
fe.2.6        08-00-20-20-32-4b   active          first learned
fe.2.9        08-00-20-77-aa-80   active          first learned
fe.2.12       00-03-ba-08-4c-f0   active          first learned
fe.2.14       00-01-f4-2c-ad-b4   active          first learned
```

Table 24-2 provides an explanation of the command output.

Table 24-2 show maclock stations Output Details

Output...	What it displays...
Port Number	Port designation. For a detailed description of possible *port_string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.
MAC address	MAC address of the end station(s) locked to the port.

Downloaded from www.Manualslib.com manuals search engine

Table 24-2 show maclock stations Output Details

Output...	What it displays...
Status	Whether the end stations are **active** or **inactive**.
State	Whether the end station locked to the port is a **first learned, first arrival** or **static** connection.

set maclock enable

Use this command to enable MAC locking on one or more ports.

Syntax

set maclock enable [*port_string*]

Parameters

port_string	(Optional) Enables MAC locking on specific port(s). For a detailed description of possible *port_string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.

Defaults

If *port_string* is not specified, MAC locking will be enabled on all ports.

Mode

Switch command, Read-Write.

Usage

MAC locking is disabled by default at device startup. Configuring one or more ports for MAC locking requires globally enabling it on the device and then enabling it on the desired ports as described in "set maclock" on page 24-6.

When enabled and configured for a specific MAC address and port string, this locks a port so that only designated end station addresses are allowed to participate in frame relay.

Example

This example shows how to enable MAC locking on fe.2.3:

```
Matrix(rw)->set maclock enable fe.2.3
```

set maclock disable

Use this command to disable MAC locking on one or more ports.

Syntax

set maclock disable [*port_string*]

Downloaded from www.Manualslib.com manuals search engine

Parameters

port_string	(Optional) Disables MAC locking on specific port(s). For a detailed description of possible *port_string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.

Defaults

If *port_string* is not specified, MAC locking will be disabled on all ports.

Mode

Switch command, Read-Write.

Example

This example shows how to disable MAC locking on fe.2.3:

```
Matrix(rw)->set maclock disable fe.2.3
```

set maclock

Use this command to create a static MAC address and enable or disable MAC locking for the specific MAC address and port.

Syntax

set maclock *mac_address port_string* {**create** | **enable** | **disable**}

Parameters

mac_address	Specifies the MAC address for which MAC locking will be created, enabled or disabled.
port_string	Specifies the port on which to create, enable or disable MAC locking. For a detailed description of possible *port_string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.
create	Establishes a MAC locking association between the specified MAC address and port. Create automatically enables MAC locking between the specified MAC address and port.
enable | **disable**	Enables or disables MAC locking between the specified MAC address and port.

Defaults

None.

Mode

Switch command, Read-Write.

Usage

Configuring one or more ports for MAC locking requires globally enabling it on the device first using the **set maclock enable** command as described in "set maclock enable" on page 24-5.

When created and enabled, this allows only the end station designated by the MAC address to participate in frame relay.

Downloaded from www.Manualslib.com manuals search engine

Example

This example shows how to create a MAC locking association between MAC address 00-a0-c9-0d-32-11 and port fe.2.3:

```
Matrix(rw)->set maclock 00-a0-c9-0d-32-11 fe.2.3 create
```

set maclock firstarrival

Use this command to restrict MAC locking on a port to a maximum number of end station addresses first connected to that port.

Syntax

set maclock firstarrival *port_string value*

Parameters

port_string	Specifies the port on which to limit MAC locking. For a detailed description of possible *port_string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.
value	Specifies the number of first arrival end station MAC addresses to be allowed connections to the port. Valid values are **0** to **600**.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to restrict MAC locking to 6 MAC addresses on fe.2.3:

```
Matrix(rw)->set maclock firstarrival fe.2.3 6
```

set maclock move

Use this command to move all current first arrival MACs to static entries.

Syntax

set maclock move *port-string*

Parameters

port-string	Specifies the port where all current first arrival MACs will be moved to static entries. For a detailed description of possible *port_string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.

Defaults

None.

Downloaded from www.Manualslib.com manuals search engine

Mode

Switch command, Read-Write.

Example

This example shows how to move all current first arrival MACs to static entries on fe.1.3:

```
Matrix(rw)->set maclock move fe.1.3
```

clear maclock firstarrival

Use this command to reset the number of first arrival MAC addresses allowed per port to the default value of 600.

Syntax

clear maclock firstarrival *port-string*

Parameters

port_string	Specifies the port on which to reset the first arrival value. For a detailed description of possible *port_string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to reset MAC first arrivals on fe.2.3:

```
Matrix(rw)->clear maclock firstarrival fe.2.3 6
```

set maclock static

Use this command to restrict MAC locking on a port to a maximum number of static (management defined) MAC addresses for end stations connected to that port.

Syntax

set maclock static *port_string value*

Parameters

port_string	Specifies the port on which to limit MAC locking. For a detailed description of possible *port_string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.
value	Specifies the number of static MAC addresses to be allowed connections to the port. Valid values are **0** to **20**.

Downloaded from www.Manualslib.com manuals search engine

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to restrict MAC locking to 4 static addresses on fe.2.3:

```
Matrix(rw)->set maclock static fe.2.3 4
```

clear maclock static

Use this command to reset the number of static MAC addresses allowed per port to the default value of 20.

Syntax

clear maclock static *port_string*

Parameters

port_string	Specifies the port on which to reset the static MAC locking limit. For a detailed description of possible *port_string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to reset static MAC locking on fe.2.3:

```
Matrix(rw)->clear maclock static fe.2.3
```

set maclock trap

Use this command to enable or disable MAC lock trap messaging.

Syntax

set maclock trap *port_string* {**enable** | **disable**}

Parameters

port_string	Specifies the port on which MAC lock trap messaging will be enabled or disabled. For a detailed description of possible *port_string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.
enable | **disable**	Enables or disables MAC lock trap messaging.

Downloaded from www.Manualslib.com manuals search engine

Defaults

None.

Mode

Switch command, Read-Write.

Usage

When enabled, this authorizes the device to send an SNMP trap message if an end station is connected that exceeds the maximum values configured using the **set maclock firstarrival** and **set maclock static** commands. Violating MAC addresses are dropped from the device's routing table.

Example

This example shows how to enable MAC lock trap messaging on fe.2.3:

```
Matrix(rw)->set maclock trap fe.2.3 enable
```

clear maclock

Use this command to clear MAC locking from one or more static MAC addresses.

Syntax

clear maclock {**all** | *mac-address port-string*}

Parameters

all	Clears all static MAC locking for one or more ports.
mac_address	Specifies the MAC address for which the MAC locking will be cleared.
port_string	Specifies the port on which to clear MAC locking. For a detailed description of possible *port_string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to clear MAC locking between MAC address 00-a0-c9-0d-32-11 and port fe.2.3:

```
Matrix(rw)->clear maclock 00-a0-c9-0d-32-11 fe.2.3
```


Downloaded from www.Manualslib.com manuals search engine

Configuring Secure Shell (SSH)

Purpose

To review, enable, disable, and configure the Secure Shell (SSH) protocol, which provides secure Telnet.

Commands

For information about...	Refer to page...
show ssh state	24-11
set ssh	24-11
set ssh hostkey	24-12
show router ssh	24-12
set router ssh	24-13
clear router ssh	24-13

show ssh state

Use this command to display the current status of SSH on the device.

Syntax

show ssh state

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Only.

Examples

This example shows how to display SSH status on the device:

```
Matrix(rw)->show ssh state
 SSH Server status:   Disabled.
```

set ssh

Use this command to enable, disable or reinitialize SSH server on the device.

Syntax

set ssh {**enable** | **disable** | **reinitialize**}

Downloaded from www.Manualslib.com manuals search engine

Parameters

enable | disable	Enables or disables SSH, or reinitializes the SSH server.
reinitialize	Reinitializes the SSH server.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to disable SSH:

```
Matrix(rw)->set ssh disable
```

set ssh hostkey

Use this command to set or reinitialize new SSH authentication keys.

Syntax

set ssh hostkey [**reinitialize**]

Parameters

reinitialize	Reinitializes the server host authentication keys.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to regenerate SSH keys:

```
Matrix(rw)->set ssh hostkey reinitialize
```

show router ssh

Use this command to display the state of SSH service to the router.

Syntax

show router ssh

Parameters

None.

Downloaded from www.Manualslib.com manuals search engine

Defaults

None.

Mode

Switch command, Read-Only.

Example

This example shows how to display the state of SSH service to the router:

```
Matrix(rw)->show router ssh
SSH Server status: Enabled
```

set router ssh

Use this command to enables or disable SSH service to the router.

Syntax

set router ssh {**enable** | **disable**}

Parameters

enable | **disable**	Enables or disable SSH service.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to disable SSH service to the router:

```
Matrix(rw)->set router ssh disable
```

clear router ssh

Use this command to reset SSH service to the router to the default state of disabled.

Syntax

clear router ssh

Parameters

None.

Defaults

None.

Downloaded from www.Manualslib.com manuals search engine

Mode

Switch command, Read-Write.

Example

This example shows how to reset SSH service to the router to the default state of disabled:

```
Matrix(rw)->clear router ssh
```


Downloaded from www.Manualslib.com manuals search engine

Configuring Access Lists



Router: These commands can be executed when the device is in **router mode** only. For details on how to enable router configuration modes, refer to "Enabling Router Configuration Modes" on page 2-103.

Purpose

To review and configure security access control lists (ACLs), which permit or deny access to routing interfaces based on protocol and source IP address restrictions.

Commands

For information about...	Refer to page...
show access-lists	24-15
access-list (standard)	24-16
access-list (extended)	24-17
ip access-group	24-20

show access-lists

Use this command to display configured IP access lists when operating in router mode.

Syntax

show access-lists [*number*]

Parameters

access-list-number	(Optional) Displays access list information for a specific access list number. Valid values are between **1** and **199**.

Defaults

If *number* is not specified, the entire table of access lists will be displayed.

Mode

Router command, Any router mode.

Example

This example shows how to display IP access list number 101. This is an extended access list, which permits or denies ICMP, UDP and IP frames based on restrictions configured with the one of the **access-list** commands. For details on configuring standard access lists, refer to "ip access-group" on page 24-20. For details on configuring extended access lists, refer to "access-list (extended)" on page 24-17.

```
Matrix>Router#show access-lists 101
Extended IP access list 101
   permit icmp host 18.2.32.130 any
   permit udp host 198.92.32.130 host 171.68.225.126 eq
```


Downloaded from www.Manualslib.com manuals search engine

```
   deny ip 150.136.0.0 0.0.255.255 224.0.0.0 15.255.255.255
   deny ip 11.6.0.0 0.1.255.255 224.0.0.0 15.255.255.255 2)
deny ip 172.24.24.0 0.0.1.255 224.0.0.0 15.255.255.255
```

access-list (standard)

Use this command to define a standard IP access list by number when operating in router mode. Restrictions defined by an access list are applied by using the **ip access-group** command ("ip access-group" on page 24-20).

Syntax

access-list *access-list-number* [**insert** | **replace** *entry*] | [**log** *1-5000* | *all*] [**move** *destination source1* [*source2*]] {**deny** | **permit**} *source* [*source-wildcard*]

no access-list *access-list-number* [*entry*]

To insert or replace an ACL entry:

access-list *access-list-number* **insert** | **replace** *entry*

To move entries within an ACL:

access-list *access-list-number* **move** *destination source1* [*source2*]

Parameters

access-list-number	Specifies a standard access list number. Valid values are from **1** to **99.**
insert | **replace** *entry*	(Optional) Inserts this new entry before a specified entry in an existing ACL, or replaces a specified entry with this new entry.
log *1-5000* | **all**	Enable syslog for ACL entry hits. Enable syslog for sequential number of ACL entry or for all ACL entries
move *destination source1 source2*	(Optional) Moves a sequence of access list entries before another entry. *Destination* is the number of the existing entry before which this new entry will be moved. *Source1* is a single entry number or the first entry number in the range to be moved. *Source2* (optional) is the last entry number in the range to be moved. If not specified, only the *source1* entry will be moved.
deny | **permit**	Denies or permits access if specified conditions are met.
protocol	Specifies an IP protocol for which to deny or permit access. Valid values and their corresponding protocols are: • **ip** - Any Internet protocol • **icmp** - Internet Control Message Protocol • **udp** - User Datagram Protocol • **tcp** - Transmission Protocol
source	Specifies the network or host from which the packet will be sent. Valid options for expressing source are: • IP address or range of addresses (A.B.C.D) • **any** - Any source host • **host** *source* - IP address of a single source host
source-wildcard	(Optional) Specifies the bits to ignore in the *source* address.

Downloaded from www.Manualslib.com manuals search engine

Defaults

- If **insert, replace** or **move** are not specified, the new entry will be appended to the access list.
- If *source2* is not specified with **move**, only one entry will be moved.

Mode

Router command, Global configuration: **Matrix>Router(config)#**

Usage

Valid *access-list-numbers* for standard ACLs are **1** to **99**. For extended ACLs, valid values are **100** to **199**.

The "no" form of this command removes the defined access list or entry.

Examples

This example shows how to allow access to only those hosts on the three specified networks. The wildcard bits apply to the host portions of the network addresses. Any host with a source address that does not match the access list statements will be rejected:

```
Matrix>Router(config)#access-list 1 permit 192.5.34.0 0.0.0.255
Matrix>Router(config)#access-list 1 permit 128.88.0.0 0.0.255.255
Matrix>Router(config)#access-list 1 permit 36.0.0.0 0.255.255.255
```

This example moves entry 16 to the beginning of ACL 22:

```
Matrix>Router(config)#access-list 22 move 1 16
```

access-list (extended)

Important Notice

Configuring extended access control lists (ACLs) is an advanced routing feature that must be enabled with a license key. If you have purchased an advanced routing license and have enabled routing on the device, you must activate your license as described in "Activating Advanced Routing Features" on page 21-1 in order to enable the extended access list command set. If you wish to purchase an advanced routing license, contact Enterasys Networks Sales.

Use this command to define an extended IP access list by number when operating in router mode.

Syntax

access-list *access-list-number* [**insert** | **replace** *entry*] | [**log** *1-5000* | **all**] [**move** *destination source1* [*source2*]] {**deny** | **permit**} *protocol source* [*source-wildcard*] [*operator* [*port*]] *destination* [*destination-wildcard*] [*operator* [*port*]] [*tos-extensions*][*icmp-type* [*icmp-code*] [**established**] [**log**]

To insert or replace an ACL entry:

access-list *access-list-number* **insert** | **replace** *entry*

To move entries within an ACL:

access-list *access-list-number* **move** *destination source1* [*source2*]

To log entries within an ACL:

access-list *access-list-number* **log** *1-5000* | **all**

Downloaded from www.Manualslib.com manuals search engine

To apply ACL restrictions to IP, UDP, or ICMP packets:

access-list *access-list-number* {**deny** | **permit**} *protocol source* [*source-wildcard*] [*operator* [*port*]] *destination* [*destination-wildcard*] [*operator* [*port*]] [*tos-extensions*][*icmp-type* [*icmp-code*] [**log**]

To apply ACL restrictions to TCP packets:

access-list *access-list-number* {**deny** | **permit**} *protocol source* [*source-wildcard*] [*operator* [*port*]] *destination* [*destination-wildcard*] [*operator* [*port*]] [*tos-extensions*][*icmp-type* [*icmp-code*] [**established**] [**log**]

no access-list *access-list-number* [*entry*]

Parameters

access-list-number	Specifies an extended access list number. Valid values are from **100** to **199**.
insert | **replace** *entry*	(Optional) Inserts this new entry before a specified entry in an existing ACL, or replaces a specified entry with this new entry.
log *1-5000* | **all**	Enable syslog for ACL entry hits. Enable syslog for sequential numbers of ACL entries or for all ACL entries.
move *destination source1 source2*	(Optional) Moves a sequence of access list entries before another entry. *Destination* is the number of the existing entry before which this new entry will be moved. *Source1* is a single entry number or the first entry number in the range to be moved. *Source2* (optional) is the last entry number in the range to be moved. If not specified, only the *source1* entry will be moved.
deny | **permit**	Denies or permits access if specified conditions are met.
protocol	Specifies an IP protocol for which to deny or permit access. Valid values and their corresponding protocols are: • 0 – 255 - Any IP protocol number, as listed in http://www.iana.org/assignments/protocol-numbers • **ip** - Any Internet protocol • **icmp** - Internet Control Message Protocol • **udp** - User Datagram Protocol • **tcp** - Transmission Protocol • **ah** - Authentication Header Protocol • **esp** - Encapsulation Security Payload • **gre** - Generic Router Encapsulation Protocol
source	Specifies the network or host from which the packet will be sent. Valid options for expressing source are: • IP address or range of addresses (A.B.C.D) • **any** - Any source host • **host** *source* - IP address of a single source host
source-wildcard	(Optional) Specifies the bits to ignore in the *source* address.

Downloaded from www.Manualslib.com manuals search engine

destination	Specifies the network or host to which the packet will be sent. Valid options for expressing destination are: • IP address (A.B.C.D) • **any** - Any destination host • **host** *source* - IP address of a single destination host
destination-wildcard	(Optional) Specifies the bits to ignore in the *destination* address.
icmp-type	(Optional) Filters ICMP frames by ICMP message type. The type is a number from **0** to **255**.
icmp-code	(Optional) Further filters ICMP frames filtered by ICMP message type by their ICMP message code. The code is a number from **0** to **255**.
operator port	(Optional) Applies access rules to TCP or UDP source or destination port numbers. Possible operands include: • **lt** *port* - Match only packets with a lower port number. • **gt** *port* - Match only packets with a greater port number. • **eq** *port* - Match only packets on a given port number. • **neq** *port* - Match only packets not on a given port number. • **range** *min-sport max-sport* - Match only packets in the range of source ports • **range** *min-dport max-dport* - Match only packets in the range of destination ports.
tos-extensions	(Optional) Applies access rules to the precedence and/or tos fields, or to the DiffServ field. That is, you can specify one or both precedence and tos fields, or you can specify the DiffServ field. Use the following keyword/value pairs to specify the tos-extensions: • precedence *value (0-7)* - Match packets based on the IP precedence value. • **tos** *value (0-15)* - Match packets based on the IP Type of Service value. • **dscp** *value (0-63)* - Match packets based on the Diffserv codepoint value.
established	(Optional) Applies TCP restrictions to established connections only.
log	(Optional) Enable the rule being configured for syslog.

Defaults

- If **insert**, **replace**, or **move** are not specified, the new entry will be appended to the access list.
- If *source2* is not specified with **move**, only one entry will be moved.
- If *icmp-type* and *icmp-code* are not specified, ICMP parameters will be applied to all ICMP message types.
- If *operator* and *port* are not specified, access parameters will be applied to all TCP or UDP ports.

Downloaded from www.Manualslib.com manuals search engine

Mode

Router command, Global configuration: **Matrix>Router(config)#**

Usage

Valid *access-list-numbers* for extended ACLs are **100** to **199**. For standard ACLs, valid values are **1** to **99**.

Restrictions defined by an access list are applied by using the **ip access-group** command as described in "ip access-group" on page 24-20.

The "no" form of this command removes the defined access list or entry.

Examples

This example shows how to define access list 101 to deny ICMP transmissions from any source and for any destination:

```
Matrix>Router(config)#access-list 101 deny ICMP any any
```

This example shows how to define access list 102 to deny TCP packets transmitted from IP source 10.1.2.1 with a port number of 42 to any destination.

```
Matrix>Router(config)#access-list 102 deny TCP host 10.1.2.1 eq 42 any
```

This example shows how to define access list 101 to deny TCP packets transmitted from any IP source port with the precedence field set to a value of 3 and the tos field set to a value of 4.

```
Matrix>Router(config)#access-list 101 deny tcp any precedence 3 tos 4
```

This example shows how to define access list 102 to deny TCP packets transmitted from any IP source port with a the DiffServ value set to 55.

```
Matrix>Router(config)#access-list 102 deny tcp any any dscp 55
```

ip access-group

Use this command to apply access restrictions to inbound or outbound frames on an interface when operating in router mode.

Syntax

ip access-group *access-list-number* {**in** | **out**}

no ip access-group *access-list-number* {**in** | **out**}

Parameters

access-list-number	Specifies the number of the access list to be applied to the access list. This is a decimal number from **1** to **199**.
in	Filters inbound frames.
out	Filters outbound frames.

Defaults

None.

Mode

Router command, Interface configuration: **Matrix>Router(config-if(Vlan <vlan_id>))#**

Downloaded from www.Manualslib.com manuals search engine

Usage

ACLs must be applied per routing interface. An entry (rule) can either be applied to inbound or outbound frames.

The “no” form of this command removes the specified access list.

Example

This example shows how to apply access list 1 for all inbound frames on VLAN 1. Through the definition of access list 1, only frames with destination 192.5.34.0 will be routed. All the frames with other destination received on VLAN 1 are dropped:

```
Matrix>Router(config)#access-list 1 permit 192.5.34.0 0.0.0.255
Matrix>Router(config)#interface vlan 1
Matrix>Router(config-if(Vlan 1))#ip access-group 1 in
```


Downloaded from www.Manualslib.com manuals search engine

Configuring Denial of Service (DoS) Prevention



Router: These commands can be executed when the device is in **router mode** only. For details on how to enable router configuration modes, refer to "Enabling Router Configuration Modes" on page 2-103.

Purpose

To configure Denial of Service (DoS) prevention, which will protect the router from attacks and notify administrators via Syslog.

Commands

For information about...	Refer to page...
show hostdos	24-22
hostdos	24-23
clear hostdos-counters	24-24

show hostdos

Use this command to display Denial of Service security status and counters.

Syntax

show hostdos

Parameters

None.

Defaults

None.

Mode

Router command, Global configuration: **Matrix>Router(config)#**

Usage

When fragmented ICMP packets protection is enabled, the Ping of Death counter will not be incremented. Ping of Death is a subset of the fragmented ICMP function.

Example

This example shows how to display Denial of Service security status and counters. For details on how to set these parameters, refer to "hostdos" on page 24-23.

```
Matrix>Router(config)#show hostdos
LAND Attack (Destination IP = Source IP)
   Disabled
Spoofed Address Check
```


Downloaded from www.Manualslib.com manuals search engine

```
   Disabled
IP packet with multicast/broadcast source address
   Always enabled
   0 attacks
Fragmented ICMP traffic
   Disabled
Large ICMP packet
   Disabled
Ping-of-Death attack
   Always enabled
   0 attacks
Port Scanning
   Disabled
```

hostdos

Use this command to enable or disable Denial of Service security features.

Syntax

hostdos {**land** | **fragmicmp** | **largeicmp** *size* | **checkspoof** | **portscan**}

no hostdos {**land** | **fragmicmp** | **largeicmp** *size* | **checkspoof**}

Parameters

land	Enables land attack protection and automatically discards illegal frames. This can be enabled globally, or per-interface.
fragmicmp	Enables fragmented ICMP and Ping of Death packets protection and automatically discards illegal frames. This can only be enabled globally.
largeicmp *size*	Enables large ICMP packets protection, specifies the packet size above which the protection starts, and automatically discards illegal frames. Valid packet size values are 1 to 65535. The default is 1024. This can only be enabled globally.
checkspoof	Enables spoofed address checking and automatically reports spoofed addresses via Syslog. This can be enabled globally, or per-interface.
portscan	Enables UDP and TCP port scan protection. This can only be enabled globally.

Defaults

None.

Mode

Router command, Global configuration: **Matrix>Router(config)#**, or
Interface configuration: **Matrix>Router(config-if(Vlan <vlan_id>))#**

Usage

The “no” form of this command disables the specified security features.

Downloaded from www.Manualslib.com manuals search engine

Examples

This example shows how to globally enable land attack and large ICMP packets protection for packets larger than 2000 bytes:

```
Matrix>Router(config)#hostdos land
Matrix>Router(config)#hostdos largeicmp 2000
```

This example shows how to enable spoofed address checking on the VLAN 1 interface:

```
Matrix>Router(config)#interface vlan 1
Matrix>Router(config-if(Vlan 1))#hostdos checkspoof
```

clear hostdos-counters

Use this command to clear Denial of Service security counters.

Syntax

clear hostdos-counters

Parameters

None.

Defaults

None.

Mode

Router command, Global configuration: **Matrix>Router(config)#**

Example

This example shows how to clear Denial of Service security counters:

```
Matrix>Router(config)#clear hostdos-counters
```


Downloaded from www.Manualslib.com manuals search engine

Configuring Flow Setup Throttling (FST)

About FST

Flow Setup Throttling (FST) is a proactive feature designed to mitigate DoS attacks before the virus can wreak havoc on the network. FST directly combats the effects of DoS attacks by limiting the number of new or established flows that can be programmed on any individual switch port. This is achieved by monitoring the new flow arrival rate and/or controlling the maximum number of allowable flows.

FST limits the vulnerability of connection attacks on the network by allowing administrators to:

- Globally enable FST on the switch and on a port-by-port basis.
- Configure the maximum flows allowed per user classification (port type) and the actions that will occur when flow limits are reached.
- Assign a user classification to each interface.
- Control the generation of SNMP notifications.
- Control the time (in seconds) to wait before generating another notification of the same type on the same interface.
- Control link status.

Purpose

To review and configure Flow Setup Throttling.

Commands

For information about...	Refer to page...
show flowlimit	24-26
set flowlimit	24-26
set flowlimit limit	24-27
clear flowlimit limit	24-28
set flowlimit action	24-28
clear flowlimit action	24-29
show flowlimit class	24-30
set flowlimit port	24-31
clear flowlimit port class	24-32
set flowlimit shutdown	24-32
set flowlimit notification	24-33
clear flowlimit notification interval	24-34
clear flowlimit stats	24-34

Downloaded from www.Manualslib.com manuals search engine

show flowlimit

Use this command to display flow setup throttling information.

Syntax

show flowlimit [**port** [*port-string*]] [**stats** [*port-string*]]

Parameters

port *port-string*	(Optional) Displays flow limiting port settings for one or all ports.
stats *port-string*	(Optional) Displays flow limiting statistics for one or all ports.

Defaults

If no optional parameters are specified, detailed flow limiting information will be displayed for all ports.

Mode

Switch command, Read-Only.

Example

This example shows how to display flow limiting information for Fast Ethernet port 1 in module 2. In this case, it is enabled for FST with an "unspecified" port classification, is currently operational, and has no FST action assigned:

```
Matrix(rw)->show flowlimit limit port fe.2.1
Flow setup throttling port configuration:

Port      Class              State    Status               Reason     Layer
--------- ------------------ -------- -------------------- ---------- -----
fe.2.1    unspecified        enabled  operational          noAction   L4
```

set flowlimit

Use this command to globally enable or disable flow setup throttling.

Syntax

set flowlimit {**enable** | **disable**}

Parameters

enable | **disable**	Globally enables or disables FST.

Defaults

None.

Mode

Switch command, Read-Write.

Downloaded from www.Manualslib.com manuals search engine

Example

This example shows how to enable FST on Fast Ethernet ports 1-5 in module 2:

```
Matrix(rw)->set flowlimit fe.2.1-5 enable
```

set flowlimit limit

Use this command to set a flow limit that will trigger an action for a port user classification.

Syntax

set flowlimit {**limit1** | **limit2** *limit*} [**userport** | **serverport** | **aggregateduser** | **interswitchlink** | **unspecified**]

Parameters

limit1 | **limit2**	Specifies this configuration as limit 1 or 2. Two limits assigned to two actions (describing what will occur when a certain flow limit is reached) can be defined per user classification.
limit	Specifies the number of flows that will trigger the associated action configuration. Valid values are **0** - **4294967295**.
userport | **serverport** | **aggregateduser** | **interswitchlink** | **unspecified**	(Optional) Assigns this limit configuration to the user classification port type: • user port • server port • aggregation port • inter-switch link • unspecified port

Defaults

If classification port type is not specified, none will be applied.

Mode

Switch command, Read-Write.

Usage

Once configured, this limit can be associated with an action using the **set flowlimit action** command as described in "set flowlimit action" on page 24-28. This limit can be assigned to one or more ports using the **set flowlimit class** command as described in "set flowlimit port" on page 24-31.

Example

This example shows how to set the flow limit 1 to 12 flows on ports classified as user ports:

```
Matrix(rw)->set flowlimit limit1 12 userport
```


Downloaded from www.Manualslib.com manuals search engine

clear flowlimit limit

Use this command to remove a flow limit configuration.

Syntax

```
clear flowlimit {limit1 | limit2} [userport | serverport | aggregateduser |
interswitchlink | unspecified]
```

Parameters

limit1 | **limit2**	Specifies the configuration to be removed as limit 1 or 2.
userport | **serverport** | **aggregateduser** | **interswitchlink** | **unspecified**	(Optional) Removes this limit configuration from the user classification port type: • user port • server port • aggregation port • inter-switch link • unspecified port

Defaults

If not specified, the limit will be removed from all port classification types.

Mode

Switch command, Read-Write.

Example

This example shows how to remove flow limit 1 from all port classifications:

```
Matrix(rw)->clear flowlimit limit1
```

set flowlimit action

Use this command to associate an action with a flow limit. This is the action that will occur once the associated flow limit is reached.

Syntax

```
set flowlimit {action1 | action2} [notify] [drop] [disable] [userport | serverport
| aggregateduser | interswitchlink | unspecified]
```

Parameters

action1 | **action2**	Specifies this configuration as action 1 or 2. Two actions describing what will occur when a certain flow limit is reached can be defined per user classification. Action number must correspond to a flow limit configured using the **set flowlimit limit** command as described in "set flowlimit limit" on page 24-27.
notify	(Optional) When flow limit is reached, generates an SNMP trap notification (if the **set flowlimit notification** function is enabled as described in "set flowlimit notification" on page 24-33).

Downloaded from www.Manualslib.com manuals search engine

drop	(Optional) When flow limit is reached, drops excess flows and discard packets.
disable	(Optional) When flow limit is reached, disables the interface (if the **set flowlimit shutdown** function is enabled as described in "set flowlimit shutdown" on page 24-32). This will clear all FST settings on the port.
userport | **serverport** | **aggregateduser** | **interswitchlink** | **unspecified**	(Optional) Assigns this action configuration to the user classification port type: • user port • server port • aggregation port • inter-switch link • unspecified port

Defaults

- If action is not specified, no action will be applied.
- If classification port type is not specified, none will be applied.

Mode

Switch command, Read-Write.

Example

This example shows how to set flow limiting action 1 to discard all flows exceeding flow limit 1 on ports classified as user ports:

```
Matrix(rw)->set flowlimit action 1 discard userport
```

clear flowlimit action

Use this command to remove a flow limiting action configuration.

Syntax

```
clear flowlimit {action1 | action2} [notify] [drop] [disable] [userport |
serverport | aggregateduser | interswitchlink | unspecified]
```

Parameters

action1 | **action2**	Specifies the configuration to be removed as action 1 or 2.
notify	(Optional) Removes the notify action.
drop	(Optional) Removes the drop action.

Downloaded from www.Manualslib.com manuals search engine

disable	(Optional) Removes the disable action.
userport | **serverport** | **aggregateduser** | **interswitchlink** | **unspecified**	(Optional) Removes this action configuration from the user classification port type: • user port • server port • aggregation port • inter-switch link • unspecified port

Defaults

- If not specified, all action types will be removed.
- If not specified, the action will be removed from all port classifications.

Mode

Switch command, Read-Write.

Example

This example shows how to remove flow limiting action 1 from all port classifications:

```
Matrix(rw)->clear flowlimit action1
```

show flowlimit class

Use this command to display flow limiting classification configuration(s).

Syntax

show flowlimit class [**userport** | **serverport** | **aggregateduser** | **interswitchlink** | **unspecified**]

Parameters

userport | **serverport** | **aggregateduser** | **interswitchlink** | **unspecified**	(Optional) Displays flow limiting information related to the following classification: • user port • server port • aggregation port • interswitch link • unspecified port

Defaults

If port classification type is not specified, information related to all classifications will be displayed.

Mode

Switch command, Read-Only.

Downloaded from www.Manualslib.com manuals search engine

Example

This example shows how to show flow limits and associated actions configured for the various port classifications:

```
Matrix(rw)->show flowlimit class
Flow setup throttling class configuration:

Class              Limit                  Action
------------------ ---------------------- ---------------------------
userPort           limit1     :800        action1    :notify
                   limit2     :1000       action2    :disable,notify

serverPort         limit1     :5000       action1    :notify
                   limit2     :6000       action2    :disable,notify

aggregatedUserPort limit1     :5000       action1    :notify
                   limit2     :6000       action2    :disable,notify

interSwitchLink    limit1     :14000      action1    :notify
                   limit2     :16000      action2    :disable,notify

unspecified        limit1     :0          action1    :notify
                   limit2     :0          action2    :disable,notify
```

set flowlimit port

Use this command to enable or disable flow limiting on one or more port(s), assign a flow limiting user classification to one or more port(s) or enable an interface previously disabled by a flow limiting action.

Syntax

set flowlimit port {**enable** | **disable**} | **class** {**userport** | **serverport** | **aggregateduser** | **interswitchlink** | **unspecified**} | **status** {**operational**} [*port-string*]

Parameters

enable | **disable**	Enables or disables flow limiting on specified ports.
class userport | **serverport** | **aggregateduser** | **interswitchlink** | **unspecified**	Assigns a user classification type to the port(s) as: • user port • server port • aggregation port • interswitch link • unspecified port
status operational	Enables an interface previously disabled by a flow limiting action.
port-string	(Optional) Specifies port(s) on which to configure flow limiting parameters.

Downloaded from www.Manualslib.com manuals search engine

Defaults

If *port-string* is not specified, settings will apply to all ports.

Mode

Switch command, Read-Write.

Usage

Once a classification is assigned, these ports will be subject to the flow limit configured (with the **set flowlimit limit** command as described in "set flowlimit limit" on page 24-27) and the action configured (with the **set flowlimit action** command as described in "set flowlimit action" on page 24-28).

Example

This example shows how to assign the user port classification type to Fast Ethernet ports 3-5 in module 2:

```
Matrix(rw)->set flowlimit port class userport fe.2.3-5
```

clear flowlimit port class

Use this command to remove flow limiting port classification properties.

Syntax

clear flowlimit port class [*port-string*]

Parameters

port-string	(Optional) Specifies port(s) on which to remove flow limiting classification properties.

Defaults

If *port-string* is not specified, classifications will be removed from all ports.

Mode

Switch command, Read-Write.

Example

This example shows how to clear port classifications from all Gigabit Ethernet ports:

```
Matrix(rw)->clear flowlimit port class ge.*.*
```

set flowlimit shutdown

Use this command to enable or disable the flow limit shut down function.

Syntax

set flowlimit shutdown {**enable** | **disable**}

Downloaded from www.Manualslib.com manuals search engine

Parameters

enable | **disable**	Enables or disables the flow limit shut down function.

Defaults

None.

Mode

Switch command, Read-Write.

Usage

When enabled, this allows ports configured with a "trap" action to send an SNMP trap message when a specified flow limit is reached.

When enabled, this allows ports configured with a "disable" action to shut down. For information on using the **set flowlimit limit** command to configure set a disable action on a port, refer to "set flowlimit limit" on page 24-27.

Example

This example shows how to enable the flow limit shut down function:

```
Matrix(rw)->set flowlimit shutdown enable
```

set flowlimit notification

Use this command to enable or disable flow limit notification, or to set a notification interval.

Syntax

set flowlimit notification {**disable** | **enable** | *interval*}

Parameters

disable | **enable**	Disables or enables SNMP notification.
interval	Specifies a notification interval (in seconds) for SNMP trap messages. Valid values are **0** - **4294967295**.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to enable the flow limit notification function:

```
Matrix(rw)->set flowlimit notification enable
```


Downloaded from www.Manualslib.com manuals search engine

clear flowlimit notification interval

Use this command to reset the SNMP flow limit notification interval to the default value of 120 seconds.

Syntax

clear flowlimit notification interval

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to reset the SNMP flow limit notification interval:

```
Matrix(rw)->clear flowlimit notification interval
```

clear flowlimit stats

Use this command to reset flow limiting statistics back to default values on one or more port(s).

Syntax

clear flowlimit stats [*port-string*]

Parameters

port-string	(Optional) Resets flow limiting statistics on specific port(s).

Defaults

If *port-string* is not specified, statistics will be reset on all ports.

Mode

Switch command, Read-Write.

Example

This example shows how to reset flow limiting statistics back to default values on Fast Ethernet port 5 in module 1:

```
Matrix(rw)->clear flowlimit stats fe.1.5
```


Downloaded from www.Manualslib.com manuals search engine

25

Authentication Configuration

This chapter describes the set of commands for supported authentication methods.

For information about...	Refer to page...
Overview of Authentication Methods	25-1
Configuring 802.1X Authentication	25-2
Configuring Port Web Authentication (PWA)	25-11
Configuring MAC Authentication	25-26
Configuring Convergence End Points (CEP) Phone Detection	25-39
RADIUS Filter-ID Attribute and Dynamic Policy Profile Assignment	25-50
Setting the Authentication Login Method	25-50
Configuring RADIUS	25-53
Configuring RFC 3580	25-60
Configuring TACACS+	25-63

Note: An Enterasys Feature Guide document that contains a complete discussion on authentication configuration exists at the following Enterasys web site: http://www.enterasys.com/support/manuals/

Overview of Authentication Methods

The following authentication methods are available for controlling which users are allowed to access, monitor, and manage the device.

- 802.1X Network Access Control — used for controlling access to network resources on a per port, per user, or per end station basis. For more details, refer to "Configuring 802.1X Authentication" on page 25-2.
- Port Web Authentication (PWA) — used for controlling access to network resources on a per user basis via HTTP. For details, refer to "Configuring Port Web Authentication (PWA)" on page 25-11.
- MAC Authentication — used for controlling access to network resources on a per MAC address basis. For details, refer to "Configuring MAC Authentication" on page 25-26.
- Convergence End Point (CEP) — Convergence Endpoint (CEP) detection is an Enterasys Networks mechanism for identifying IP phones that are connected to a given switch. When an endpoint is discovered, a policy is then assigned to the endpoint. For details, refer to "Configuring Convergence End Points (CEP) Phone Detection" on page 25-39.

Downloaded from www.Manualslib.com manuals search engine

- Local user credentials — used for local authentication and authorization of CLI and WebView management sessions. For details, refer to "Setting User Accounts and Passwords" on page 2-15 and "Setting the Authentication Login Method" on page 25-50.
- Remote AAA service — used for remote authentication, authorization, and accounting of CLI and WebView management sessions, as well as all network access sessions provisioned by way of 802.1x, PWA, or MAC Authentication. For details, refer to "Setting the Authentication Login Method" on page 25-50 and "Configuring 802.1X Authentication" on page 25-2.
- Support for RADUIS, RFC 3580, and TACACS+ can be found in the following sections: "Configuring RADIUS" on page 25-53, "Configuring RFC 3580" on page 25-60, and "Configuring TACACS+" on page 25-63

Configuring 802.1X Authentication

About Multi-User Authentication

Enterasys Networks' enhanced version of the IEEE 802.1X-2001 specification decreases security vulnerabilities inherent with the standard implementation, and allows multiple devices and users, also known as "supplicants," to be authenticated on a single port. The enhanced standard clearly distinguishes each network access port from its access "entities," which maintain authentication instructions associated with each unique potential supplicant.

802.1X enhancements are backwards-compatible with existing 802.1X supplicants and configurations, and are designed to seamlessly integrate into Enterasys' per-user policy management system; allowing much more granular control over user authorization.

The Enterasys multi-user 802.1X implementation includes the following components:

- A Multi-Mode Enabled Enterasys Matrix System—only when a system is set to operate in multiple authentication mode (as described in "Configuring Multiple Authentication" on page 27-1) can the enhanced 802.1X feature be used. The system's ports intended for network access to authenticate and authorize supplicants will be allowed to simultaneously utilize more than one access entity.
- Access Entities—responsible for maintaining state, counters, and statistics for an individual supplicant. An access entity is activated from a pool of configured access entities when a potential supplicant on a port needs to be authenticated. It becomes deactivated when the supplicant logs off, cannot be authenticated, or the Enterasys Matrix device determines that the supplicant or associated policy settings are no longer valid.
- Supplicants—devices or users that desire access to the network, such as workstations, printers, PDAs, or hard-wired or wireless phones. These will be identified by the system using a combination of connection port, MAC addresses, and allocated access entity index. Once a supplicant is successfully authenticated, the system is responsible for enforcing the degree to which the supplicant will be authorized to access the network, using information sent to it by the authentication server.
- Authentication Server—typically a RADIUS authority, where the Enterasys Matrix system and server have mutually-configured knowledge of one another.

Purpose

To review and configure 802.1X authentication for one or more ports using EAPOL (Extensible Authentication Protocol). 802.1X controls network access by enforcing user authorization on

Downloaded from www.Manualslib.com manuals search engine

selected ports, which results in allowing or denying network access according to RADIUS server configuration.

Commands

For information about...	Refer to page...
show dot1x	25-3
show dot1x auth-config	25-5
set dot1x	25-7
set dot1x auth-config	25-7
clear dot1x auth-config	25-9

show dot1x

Use this command to display 802.1X status, diagnostics, statistics, and reauthentication or initialization control information for one or more ports.

Syntax

show dot1x [**auth-config** | **access-entity** | **auth-diag** | **auth-session-stats auth-stats** [**all**] [*port-string*] [**index** *index-list*] | [**mac** [**all**] *mac* [*port-string*] [**index** *index-list*] | [**port** [**init** | **reauth**]] [*port-string*]]

Parameters

auth-config	(Optional) Displays authentication configuration information.
access-entity	(Optional) Displays access entity information.
auth-diag	(Optional) Displays authentication diagnostics information.
auth-session-stats	(Optional) Displays authentication session statistics.
auth-stats	(Optional) Displays authentication statistics.
all	(Optional) Displays inactive and active authentication entries.
mac all *mac*	Displays information for one or all MAC addresses.
index *index-list*	(Optional) Displays information for one or more access entities. Valid values are 0 - 8191.
port init | **reauth**	(Optional) Displays the status of port initialization and reauthentication control.
port-string	(Optional) Displays information for specific port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.

Defaults

- If no parameters are specified, 802.1X status will be displayed.
- If **all** is not specified, only active entries will be displayed.
- If *index* is not specified, information for all access entities will be displayed.
- If *port-string* is not specified, information for all ports will be displayed.

Downloaded from www.Manualslib.com manuals search engine

Mode

Switch command, Read-Only.

Examples

This example shows how to display 802.1X status:

```
Matrix(rw)->show dot1x
DOT1X is disabled.
```

This example shows how to display authentication diagnostics information for fe.1.1:

```
Matrix(rw)->show dot1x auth-diag fe.1.1

 Port: 1     Auth-Diag:
 Enter Connecting:                    0
 EAP Logoffs While Connecting:        0
 Enter Authenticating:                0
 Success While Authenticating:        0
 Timeouts While Authenticating:       0
 Fail While Authenticating:           0
 ReAuths While Authenticating:        0
 EAP Starts While Authenticating:     0
 EAP Logoff While Authenticating:     0
 ReAuths While Authenticated:         0
 EAP Starts While Authenticated:      0
 EAP Logoff While Authenticated:      0
 Backend Responses:                   0
 Backend Access Challenges:           0
 Backend Other Requests To Supp:      0
 Backend NonNak Responses From Supp:  0
 Backend Auth Successes:              0
 Backend Auth Fails:                  0
```

This example shows how to display authentication session statistics for fe.1.1:

```
Matrix(rw)->show dot1x auth-session-stats fe.1.1

 Port: 1     Auth-Session-Stats:
 Session Octets Rx:        0
 Session Octets Tx:        0
 Session Frames Rx:        0
 Session Frames Tx:        0
 Session Id:               (1, 00-00-00-00-00-00)
 Session Authentic Method: Remote Auth Server
 Session Time:             0 secs
 Session Terminate Cause:  Port Failure
 Session UserName:
```

This example shows how to display authentication statistics for fe.1.1:

Downloaded from www.Manualslib.com manuals search engine

```
Matrix(rw)->show dot1x auth-stats fe.1.1

 Port: 1     Auth-Stats:
 EAPOL Frames Rx:            0
 EAPOL Frames Tx:            0
 EAPOL Start Frames Rx:      0
 EAPOL Logoff Frames Rx:     0
 EAPOL RespId Frames Rx:     0
 EAPOL Resp Frames Rx:       0
 EAPOL ReqId Frames Tx:      0
 EAPOL Req Frames Tx:        0
 Invalid EAPOL Frames Rx:    0
 EAP Length Error Frames Rx: 0
 Last EAPOL Frame Version:   0
 Last EAPOL Frame Source:    0:0:0:0:0:0
```

show dot1x auth-config

Use this command to display 802.1X authentication configuration settings for one or more ports.

Syntax

show dot1x auth-config [**authcontrolled-portcontrol**] [**keytxenabled**] [**maxreq**] [**quietperiod**] [**reauthenabled**] [**reauthperiod**] [**servertimeout**] [**supptimeout**] [**txperiod**] [*port-string*]

Parameters

authcontrolled-portcontrol	(Optional) Displays the current value of the controlled Port control parameter for the Port.
keytxenabled	(Optional) Displays the state of 802.1X key transmission currently in use by the authenticator PAE state machine.
maxreq	(Optional) Displays the value set for maximum requests currently in use by the backend authentication state machine.
quietperiod	(Optional) Displays the value set for quiet period currently in use by the authenticator PAE state machine.
reauthenabled	(Optional) Displays the state of reauthentication control used by the Reauthentication Timer state machine.
reauthperiod	(Optional) Displays the value, in seconds, set for the reauthentication period used by the reauthentication timer state machine.
servertimeout	(Optional) Displays the server timeout value, in seconds, currently in use by the backend authentication state machine.
supptimeout	(Optional) Displays the authentication supplicant timeout value, in seconds, currently in use by the backend authentication state machine.

Downloaded from www.Manualslib.com manuals search engine

txperiod	(Optional) Displays the transmission period value, in seconds, currently in use by the authenticator PAE state machine.
port-string	(Optional) Limits the display of desired information information to specific port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.

Defaults

- If no parameters are specified, all 802.1X settings will be displayed.
- If *port-string* is not specified, information for all ports will be displayed.

Mode

Switch command, Read-Only.

Examples

This example shows how to display the EAPOL port control mode for fe.1.1:

```
Matrix(rw)->show dot1x auth-config authcontrolled-portcontrol fe.1.1
Port 1: Auth controlled port control:             Auto
```

This example shows how to display the 802.1X quiet period settings for fe.1.1:

```
Matrix(rw)->show dot1x auth-config quietperiod fe.1.1
 Port 1: Quiet period:         30
```

This example shows how to display all 802.1X authentication configuration settings for fe.2.24:

```
Matrix(rw)->show dot1x fe.2.24
Port: fe.2.24    Auth-Config:
PAE state                              : Initialize
Backend auth State                     : Initialize
Admin controlled directions            : Both
Oper controlled directions             : Both
Auth controlled port status            : Unauthorized
Auth controlled port control           : Auto
Quiet period                           : 60 seconds
Tx period                              : 30 seconds
Supp Timeout                           : 30 seconds
Server Timeout                         : 30 seconds
Max requests                           : 2
Reauthentication period                : 3600 seconds
Reauthentication enabled               : FALSE
Key tx enabled                         : FALSE
```


Downloaded from www.Manualslib.com manuals search engine

set dot1x

Use this command to enable or disable 802.1X authentication, to reauthenticate one or more access entities, or to reinitialize one or more supplicants.

Syntax

set dot1x {[**enable** | **disable**] [**init** | **reauth** [*port-string*] [**index** *index-list*]}

Parameters

enable | **disable**	Enables or disables 802.1X.
init | **reauth**	Reinitializes one or more access entities or reauthenticates one or more supplicants.
port-string	(Optional) Specifies the port(s) to reinitialize or reauthenticate.
index *index-list*	(Optional) Specifies one or more access entities on which to enable initialization or reauthentication control. Valid values are **0** - **8191**.

Defaults

If not specified, the reinitialization or reauthentication setting will be applied to all ports.

If *index* is not specified, all access entities will be affected.

Mode

Switch command, Read-Write.

Examples

This example shows how to enable 802.1X:

```
Matrix(rw)->set dot1x enable
```

This example shows how to reinitialize fe.2.24:

```
Matrix(rw)->set dot1x init fe.2.24
```

set dot1x auth-config

Use this command to configure 802.1X authentication.

Syntax

set dot1x auth-config {[**authcontrolled-portcontrol** {**auto** | **forced-auth** | **forced-unauth**}] [**keytxenabled**{**false** | **true**}] [**maxreq** *value*] [**quietperiod** *value*] [**reauthenabled** {**false** | **true**}] [**reauthperiod** *value*] [**servertimeout** *timeout*] [**supptimeout** *timeout*] [**txperiod** *value*]} [*port-string*]

Downloaded from www.Manualslib.com manuals search engine

Parameters

authcontrolled-portcontrol auto | **forced-auth** | **forced-unauth**	Specifies the EAPOL port control mode as: • **auto** - Auto authorization mode (default). The Enterasys Matrix system will only forward frames received on a port which are considered authenticated according to the state of the corresponding access entity. • **forced-auth** - Forced authorized mode, which effectively disables 802.1X authentication on the port, and allows all frames received on the port to be forwarded. • **forced-unauth** - Forced unauthorized mode, which effectively disables 802.1X authentication on the port. When 802.1X is the only active authentication agent on a given port, this setting means all frames received will be dropped.
keytxenabled false | **true**	Enables (**true**) or disables (**false**) 802.1X key transmission by the authenticator PAE state machine.
maxreq *value*	Specifies the maximum number of authentication requests allowed by the backend authentication state machine. Valid values are **1** - **10**.
quietperiod *value*	Specifies the time (in seconds) following a failed authentication before another attempt can be made by the authenticator PAE state machine. Valid values are **0** - **65535**.
reauthenabled false | **true**	Enables (**true**) or disables (**false**) reauthentication control of the reauthentication timer state machine.
reauthperiod *value*	Specifies the time lapse (in seconds) between attempts by the reauthentication timer state machine to reauthenticate a port. Valid values are **0** - **65535**.
servertimeout *timeout*	Specifies a timeout period (in seconds) for the authentication server, used by the backend authentication state machine. Valid values are **1** - **300**.
supptimeout *timeout*	Specifies a timeout period (in seconds) for the authentication supplicant used by the backend authentication state machine. Valid values are **1** - **300**.
txperiod *value*	Specifies the period (in seconds) which passes between authenticator PAE state machine EAP transmissions. Valid values are **1** - **65535**.
port-string	(Optional) Limits the configuration of desired settings to specified port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.

Defaults

If *port-string* is not specified, authentication parameters will be set on all ports

Mode

Switch command, Read-Write.

Examples

This example shows how to set EAPOL port control to forced authorized mode on ports fe.1.1-5, which disables authentication on these ports:

```
Matrix(rw)->set dot1x auth-config authcontrolled-portcontrol forced-auth fe.1.1-5
```


Downloaded from www.Manualslib.com manuals search engine

This example shows how to enable reauthentication control on ports fe.1.1-3:

```
Matrix(rw)->set dot1x auth-config reathenabled true fe.1.1-3
```

This example shows how to set the 802.1X quiet period to 120 seconds on ports fe.1.1-3:

```
Matrix(rw)->set dot1x auth-config quietperiod 120 fe.1.1-3
```

clear dot1x auth-config

Use this command to reset 802.1X authentication parameters to default values on one or more ports.

Syntax

clear dot1x auth-config [**authcontrolled-portcontrol**] [**keytxenabled**] [**maxreq**] [**quietperiod**] [**reauthenabled**] [**reauthperiod**] [**servertimeout**] [**supptimeout**] [**txperiod**] [*port-string*]

Parameters

authcontrolled-portcontrol	(Optional) Resets the 802.1X port control mode to **auto**.
keytxenabled	(Optional) Resets the 802.1X key transmission state to disabled (**false**).
maxreq	(Optional) Resets the maximum requests value to **2**.
quietperiod	(Optional) Resets the quiet period value to **60** seconds.
reauthenabled	(Optional) Resets the reauthentication control state to disabled (**false**).
reauthperiod	(Optional) Resets the reauthentication period value to 3**600** seconds.
servertimeout	(Optional) Resets the server timeout value to **30** seconds.
supptimeout	(Optional) Resets the authentication supplicant timeout value to **30** seconds.
txperiod	(Optional) Resets the transmission period value to **30** seconds.
port-string	(Optional) Resets settings on specific port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.

Defaults

- If no parameters are specified, all authentication parameters will be reset.
- If *port-string* is not specified, parameters will be set on all ports.

Mode

Switch command, Read-Write.

Examples

This example shows how to reset the 802.1X port control mode to auto on all ports:

```
Matrix(rw)->clear dot1x auth-config authcontrolled-portcontrol
```

This example shows how to reset reauthentication control to disabled on ports fe.1.1-3:

```
Matrix(rw)->clear dot1x auth-config reauthenabled fe.1.1-3
```

This example shows how to reset the 802.1X quiet period to 60 seconds on ports fe.1.1-3:

Downloaded from www.Manualslib.com manuals search engine

```
Matrix(rw)->clear dot1x auth-config quietperiod fe.1.1-3
```


Downloaded from www.Manualslib.com manuals search engine

Configuring Port Web Authentication (PWA)

About PWA

PWA provides a way of authenticating users before allowing general access to the network. A PWA user's access to the network is restricted until after the user successfully logs in via a web browser using the Enterasys Matrix Series web-based security interface. The Enterasys Matrix Series device will validate all login credential from the user with a RADIUS server before allowing network access.

PWA is an alternative to 802.1X and MAC authentication. It allows only the essential protocols and services required by the authentication process between the end-station and the network. All other traffic is discarded. When a user is in the unauthenticated state, any user traffic requesting network resources will not be allowed.

To log on using PWA, the user makes a request via a web browser for the PWA web page or is automatically redirected to this login page after requesting a URL in a browser.

Depending upon the authenticated state of the user, a login page or a logout page will display. When a user submits username and password, the switch then authenticates the user via a preconfigured RADIUS server. If the login is successful, then the user will be granted full network access according to the user's policy configuration on the switch.

PWA Configuration Considerations

In order to optimize PWA authentication on the Enterasys Matrix Series device, the device must be configured to satisfy the minimum requirements of an authenticating client needing to send an HTTP request with its web browser. Typically, the client will need DNS and ARP resolution before it can generate the HTTP request needed to do a PWA login. Also, DHCP may be needed in many environments. These services are not provided by PWA and must be provided by the network. To accomplish this, the device must be configured to allow access to the needed services.

The first step is to make sure that the multiple authentication port mode settings are set to "auth-opt" on all ports that are configured to run PWA.

Examples

This example shows how to set the multiple authentication port mode to "auth-opt" for all Fast Ethernet ports in the chassis or standalone device:

```
Matrix(rw)->set multiauth port mode auth-opt fe.*.*
```

For details on using the **set multiauth port** command, refer to "set multiauth port" on page 27-6.

Setting the port mode in this fashion will allow traffic to flow through the port without authentication according to its configuration. By default, this would allow all traffic to be forwarded. Conversely, you could configure the ports to drop all traffic, but this is not the most effective solution. Better yet would be to configure the port to provide only the minimal services and nothing more. The most powerful tool for accomplishing this goal is policy configuration. Policies provide the flexibility needed to tailor these services to the configuration and security needs of your environment.

This example shows how to configure a policy profile that will discard all traffic by default:

```
Matrix(rw)->set policy profile 1 name "Unauthenticated User" pvid 0 pvid-status
enable
```

This example shows how to configure policy profile rule 1 that will enable the selective services required for PWA. This rule will:

- forward ARP requests,

Downloaded from www.Manualslib.com manuals search engine

- allow access to a server (at IP 1.2.3.4) that acts as both a DNS and DHCP server, and
- be assigned as the default policy profile for all Fast Ethernet ports.

```
Matrix(rw)->set policy rule 1 ether 0x806 forward
Matrix(rw)->set policy rule 1 ipdest 1.2.3.4 forward
Matrix(rw)->set policy rule 1 udpdest 67 forward
Matrix(rw)->set policy rule 1 updsource 68 forward
Matrix(rw)->set policy port fe.*.* 1
```

Also, the PWA client must be configured (statically, or through DHCP) to have routes to both the resolved URL (a local route, or an actual gateway) and the PWA IP address. DHCP may be configured to explicitly return a static route for the client, or to inform the client that all routes are local (meaning the client is its own default gateway).

For more information on configuring policy profiles, refer to Chapter 8.

For more information on configuring DHCP, refer to "DHCP Overview" on page 20-1.

Purpose

To review, enable, disable, and configure Port Web Authentication (PWA).

Commands

For information about...	Refer to page...
show pwa	25-13
set pwa	25-15
set pwa hostname	25-15
clear pwa hostname	25-16
show pwa banner	25-16
set pwa banner	25-17
set pwa displaylogo hide	25-17
clear pwa banner	25-17
set pwa displaylogo	25-18
set pwa redirecttime	25-18
set pwa ipaddress	25-19
set pwa protocol	25-19
set pwa enhancedmode	25-20
set pwa guestname	25-21
clear pwa guestname	25-21
set pwa guestpassword	25-22
set pwa gueststatus	25-22
set pwa initialize	25-23
set pwa quietperiod	25-23

Downloaded from www.Manualslib.com manuals search engine

For information about...	Refer to page...
set pwa maxrequests	25-24
set pwa portcontrol	25-24
show pwa session	25-25

show pwa

Use this command to display port web authentication information for one or more ports.

Syntax

show pwa [*port-string*]

Parameters

port-string	(Optional) Displays PWA information for specific port(s).

Defaults

If *port-string* is not specified, PWA information will be displayed for all ports.

Mode

Switch command, Read-Only.

Examples

This example shows how to display PWA information for ge.2.1:

```
Matrix(rw)->show pwa ge.2.1
PWA Status                  - enabled
PWA IP Address              - 192.168.62.99
PWA Protocol                - PAP
PWA Enhanced Mode           - N/A
PWA Logo                    - enabled
PWA Guest Networking Status - disabled
PWA Guest Name              - guest
PWA Redirect Time           - N/A

Port     Mode              AuthStatus      QuietPeriod  MaxReq
-------- ----------------  --------------  -----------  ---------
ge.2.1   foreauthorized    disconnected    60           16
```

Table 25-1 provides an explanation of the command output.

Downloaded from www.Manualslib.com manuals search engine

Table 25-1 show pwa Output Details

Output...	What it displays...
PWA Status	Whether or not port web authentication is enabled or disabled. Default state of disabled can be changed using the **set pwa** command as described in "set pwa" on page 25-15.
PWA IP Address	IP address of the end station from which PWA will prevent network access until the user is authenticated. Set using the **set pwa ipaddress** command as described in "set pwa ipaddress" on page 25-19.
PWA Protocol	Whether PWA protocol is CHAP or PAP. Default setting of PAP can be changed using the set pwa protocol command as described in "set pwa protocol" on page 25-19.
PWA Enhanced Mode	Whether PWA enhanced mode is enabled or disabled. Default state of disabled can be changed using the **set pwa enhancedmode** command as described in "set pwa enhancedmode" on page 25-20.
PWA Logo	Whether the Enterasys Networks logo will be displayed or hidden at user login. Default state of enabled (displayed) can be changed using the **set pwa displaylogo** command as described in "set pwa displaylogo" on page 25-18.
PWA Guest Networking Status	Whether PWA guest user status is disabled or enabled with RADIUS or no authentication. Default state of disabled can be changed using the **set pwa gueststatus** command as described in "set pwa gueststatus" on page 25-22.
PWA Guest Name	Guest user name for PWA enhanced mode networking. Default value of "guest" can be changed using the **set pwa guestname** command as described in "set pwa guestname" on page 25-21.
PWA Guest Password	Guest user's password. Default value of an empty string can be changed using the **set pwa guestpassword** command as described in "set pwa guestpassword" on page 25-22.
PWA Redirect Time	Time in seconds after login success before the user is redirected to the PWA home page. Default of 5 can be reset using the **set pwa redirecttime** command as described in "set pwa redirecttime" on page 25-18.
Port	PWA port designation.
Mode	PWA port control mode.
Auth Status	Whether or not the port state is disconnected, authenticating authenticated, or held (authentication has failed).
Quiet Period	Amount of time a port will be in the held state after a user unsuccessfully attempts to log on to the network. Default value of 60 can be changed using the **set pwa quietperiod** command as described in "set pwa quietperiod" on page 25-23.
MaxReq	Maximum number of log on attempts allowed before transitioning the port to a held state. Default value of 2 can be changed using the **set pwa maxrequests** command as described in "set pwa maxrequests" on page 25-24.

Downloaded from www.Manualslib.com manuals search engine

set pwa

Use this command to enable or disable port web authentication.

Syntax

set pwa {**enable** | **disable**}

Parameters

enable | **disable**	Enables or disables port web authentication.

Defaults

None.

Mode

Switch command, Read-Write.

Usage

Port Web Authentication cannot be enabled if either MAC authentication or EAPOL (802.1X) is enabled. For information on disabling 802.1X, refer to "set dot1x" on page 25-7. For information on disabling MAC authentication, refer to "set macauthentication" on page 25-29.

Example

This example shows how to enable port web authentication:

```
Matrix(rw)->set pwa enable
```

set pwa hostname

Use this command to set a port web authentication host name.

Syntax

set pwa hostname *name*

Parameters

name	Specifies a name for accessing the PWA login page.

Defaults

None.

Mode

Switch command, Read-Write.

Usage

This is a URL for accessing the PWA login page.

Downloaded from www.Manualslib.com manuals search engine

Example

This example shows how to set the PWA host name to “pwahost”:

```
Matrix(rw)->set pwa hostname pwahost
```

clear pwa hostname

Use this command to clear the port web authentication host name.

Syntax

clear pwa hostname

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to clear the PWA host name:

```
Matrix(rw)->clear pwa hostname
```

show pwa banner

Use this command to display the port web authentication login banner string.

Syntax

show pwa banner

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Only.

Example

This example shows how to display the PWA login banner:

```
Matrix(rw)->show pwa banner
Welcome to Enterasys Networks
```


Downloaded from www.Manualslib.com manuals search engine

set pwa banner

Use this command to configure a string to be displayed as the PWA login banner.

Syntax

set pwa banner *string*

Parameters

string	Specifies the PWA login banner.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to set the PWA login banner to "Welcome to Enterasys Networks":

```
Matrix(rw)->set pwa banner "Welcome to Enterasys Networks"
```

set pwa displaylogo hide

Use this command to disable the currently configured PWA banner.

Syntax

set pwa displaylogo hide

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example disables the current PWA login banner:

```
Matrix(rw)->set pwa displaylogo hide
```

clear pwa banner

Use this command to reset the PWA login banner to a blank string.

Syntax

clear pwa banner

Downloaded from www.Manualslib.com manuals search engine

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to reset the PWA login banner to a blank string

```
Matrix(rw)->clear pwa banner
```

set pwa displaylogo

Use this command to set the display options for the Enterasys Networks logo.

Syntax

set pwa displaylogo {**display** | **hide**}

Parameters

display | **hide**	Displays or hides the Enterasys Networks logo when the PWA website displays.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to hide the Enterasys Networks logo:

```
Matrix(rw)->set pwa displaylogo hide
```

set pwa redirecttime

Use this command to set the PWA login success page redirect time.

Syntax

set pwa redirecttime *time*

Parameters

time	Specifies the number of seconds before the user will be redirected to the PWA home page after successful login. Valid values are **0** - **120**.

Downloaded from www.Manualslib.com manuals search engine

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to set the PWA redirect time to 10 seconds:

```
Matrix(rw)->set pwa redirecttime 10
```

set pwa ipaddress

Use this command to set the PWA IP address.

Syntax

set pwa ipaddress *ip-address*

Parameters

ip-address	Specifies a globally unique IP address. This same value must be configured into every authenticating switch in the domain.

Defaults

None.

Mode

Switch command, Read-Write.

Usage

This is the IP address of the end station from which PWA will prevent network access until the user is authenticated.

Example

This example shows how to set a PWA IP address of 1.2.3.4:

```
Matrix(rw)->set pwa ipaddress 1.2.3.4
```

set pwa protocol

Use this command to set the port web authentication protocol.

Syntax

set pwa protocol {**chap** | **pap**}

Downloaded from www.Manualslib.com manuals search engine

Parameters

chap | **pap**	Sets the PWA protocol to: • CHAP (PPP Challenge Handshake Protocol) - encrypts the username and password between the end-station and the switch port. • PAP (Password Authentication Protocol- does not provide any encryption between the end-station the switch port.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to set a the PWA protocol to CHAP:

```
Matrix(rw)->set pwa protocol chap
```

set pwa enhancedmode

Use this command to enable or disable PWA enhanced mode.

Syntax

set pwa enhancedmode {**enable** | **disable**}

Parameters

enable | **disable**	Enables or disables PWA enhanced mode.

Defaults

None.

Mode

Switch command, Read-Write.

Usage

When enabled, users on unauthenticated PWA ports can type any URL into a browser and be presented the PWA login page on their initial web access. They will also be granted guest networking privileges.

Example

This example shows how to enable PWA enhanced mode:

```
Matrix(rw)->set pwa enhancedmode enable
```


Downloaded from www.Manualslib.com manuals search engine

set pwa guestname

Use this command to set a guest user name for PWA enhanced mode networking.

Syntax

set pwa guestname *name*

Parameters

name	Specifies a guest user name.

Defaults

None.

Mode

Read-Write.

Usage

When enhanced mode is enabled (as described in "set pwa enhancedmode" on page 25-20), PWA will use this name to grant network access to guests without established login names and passwords.

Example

This example shows how to set the PWA guest user name to "guestuser":

```
Matrix(rw)->set pwa guestname guestuser
```

clear pwa guestname

Use this command to clear the PWA guest user name.

Syntax

clear pwa guestname

Parameters

None.

Defaults

None.

Mode

Read-Write.

Example

This example shows how to clear the PWA guest user name

```
Matrix(rw)->clear pwa guestname
```


Downloaded from www.Manualslib.com manuals search engine

set pwa guestpassword

Use this command to set the guest user password for PWA networking.

Syntax

set pwa guestpassword

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Write.

Usage

When enhanced mode is enabled, (as described in "set pwa enhancedmode" on page 25-20) PWA will use this password and the guest user name to grant network access to guests without established login names and passwords.

Example

This example shows how to set the PWA guest user password name:

```
Matrix(rw)->set pwa guestpasword
Guest Password: *********
Retype Guest Password: *********
```

set pwa gueststatus

Use this command to enable or disable guest networking for port web authentication.

Syntax

set pwa gueststatus {**authnone** | **authradius** | **disable**}

Parameters

authnone	Enables guest networking with no authentication method.
authradius	Enables guest networking with RADIUS authentication. Upon successful authentication from RADIUS, PWA will apply the policy returned from RADIUS to the PWA port.
disable	Disables guest networking.

Defaults

None.

Mode

Read-Write.

Downloaded from www.Manualslib.com manuals search engine

Usage

When enhanced mode is enabled (as described in "set pwa enhancedmode" on page 25-20), PWA will use a guest password and guest user name to grant network access with default policy privileges to users without established login names and passwords.

Example

This example shows how to enable PWA guest networking with RADIUS authentication:

```
Matrix(rw)->set pwa guestnetworking authradius
```

set pwa initialize

Use this command to initialize a PWA port to its default unauthenticated state.

Syntax

set pwa initialize [*port-string*]

Parameters

port-string	(Optional) Initializes specific port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.

Defaults

If *port-string* is not specified, all ports will be initialized.

Mode

Read-Write.

Example

This example shows how to initialize ports fe.1.5-7:

```
Matrix(rw)->set pwa initialize fe.1.5-7
```

set pwa quietperiod

Use this command to set the amount of time a port will remain in the held state after a user unsuccessfully attempts to log on to the network.

Syntax

set pwa quietperiod *time* [*port-string*]

Parameters

time	Specifies quiet time in seconds.
port-string	(Optional) Sets the quiet period for specific port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.

Downloaded from www.Manualslib.com manuals search engine

Defaults

If *port-string* is not specified, quiet period will be set for all ports.

Mode

Read-Write.

Example

This example shows how to set the PWA quiet period to 30 seconds for ports fe.1.5-7:

```
Matrix(rw)->set pwa quietperiod 30 fe.1.5-7
```

set pwa maxrequests

Use this command to set the maximum number of log on attempts allowed before transitioning the PWA port to a held state.

Syntax

set pwa maxrequests *maxrequests* [*port-string*]

Parameters

maxrequests	Specifies the maximum number of log on attempts.
port-string	(Optional) Sets the maximum requests for specific port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.

Defaults

If *port-string* is not specified, maximum requests will be set for all ports.

Mode

Read-Write.

Example

This example shows how to set the PWA maximum requests to 3 for all ports:

```
Matrix(rw)->set pwa maxrequests 3
```

set pwa portcontrol

Use this command to set the PWA port control mode.

Syntax

set pwa portcontrol {**enable** | **disable**} [*port-string*]

Downloaded from www.Manualslib.com manuals search engine

Parameters

enable | **disable**	Enables or disables PWA on the specified port.
port-string	(Optionally) Enables or disables a specific port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.

Defaults

Enables or disables all ports if no port is specified.

Mode

Switch command, Read-Write.

Example

This example shows how to enable PWA on all ports:

```
Matrix(rw)->set pwa portcontrol enable
```

show pwa session

Use this command to display information about current PWA sessions.

Syntax

show pwa session [*port-string*]

Parameters

port-string	(Optional) Displays PWA session information for specific port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.

Defaults

If *port-string* is not specified, session information for all ports will be displayed.

Mode

Read-Only.

Example

This example shows how to display PWA session information:

```
Matrix(rw)->show pwa session
Port     MAC               IP              User          Duration     Status
-------- ----------------- --------------- ------------- ------------ ---------
ge.2.19  00-c0-4f-20-05-4b 172.50.15.121   pwachap10     0,14:46:55   active
ge.2.19  00-c0-4f-24-51-70 172.50.15.120   pwachap1      0,15:43:30   active
ge.2.19  00-00-f8-78-9c-a7 172.50.15.61    pwachap11     0,14:47:58   active
```


Downloaded from www.Manualslib.com manuals search engine

Configuring MAC Authentication

Purpose

To review, disable, enable and configure MAC authentication. This allows the device to authenticate source MAC addresses in an exchange with an authentication server. The authenticator (switch) selects a source MAC seen on a MAC-authentication enabled port, and submits it to a backend client for authentication. The backend client uses the MAC address stored password, if required, as credentials for an authentication attempt. If accepted, a string representing an access policy may be returned. If present, the switch applies the associated policy rules. For an information on configuring policy classification, refer back to Chapter 8.

Commands

For information about...	Refer to page...
show macauthentication	25-26
show macauthentication session	25-28
set macauthentication	25-29
set macauthentication password	25-29
clear macauthentication password	25-30
set macauthentication significant-bits	25-30
clear macauthentication significant-bits	25-31
set macauthentication port	25-31
set macauthentication authallocated	25-32
clear macauthentication authallocated	25-32
set macauthentication portinitialize	25-33
set macauthentication macinitialize	25-33
set macauthentication reauthentication	25-34
set macauthentication portreauthenticate	25-34
set macauthentication macreauthenticate	25-35
set macauthentication reauthperiod	25-35
clear macauthentication reauthperiod	25-36
set macauthentication quietperiod	25-37
clear macauthentication quietperiod	25-37

show macauthentication

Use this command to display MAC authentication information for one or more ports.

Syntax

show macauthentication [*port-string*]

Downloaded from www.Manualslib.com manuals search engine

Parameters

port-string	(Optional) Displays MAC authentication information for specific port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.

Defaults

If *port-string* is not specified, MAC authentication information will be displayed for all ports.

Mode

Switch command, Read-Only.

Examples

This example shows how to display MAC authentication information for ge.1.1 through 8:

```
Router3(su)->show macauthentication ge.1.1-8
MAC authentication:           - disabled
MAC user password:            - NOPASSWORD
Port username significant bits  - 48

 Port      Port     Quiet      Reauth     Auth     Auth        Reauthentications
           State    Period     Period     Allowed  Allocated
 --------  -------- ---------- ---------- -------- ---------   ---------------
 ge.1.1    disabled   0          3600       256      256        disabled
 ge.1.2    disabled   0          3600       256      256        disabled
 ge.1.3    disabled   0          3600       256      256        disabled
 ge.1.4    disabled   0          3600       256      256        disabled
 ge.1.5    disabled   0          3600       256      256        disabled
 ge.1.6    disabled   0          3600       256      256        disabled
 ge.1.7    disabled   0          3600       256      256        disabled
 ge.1.8    disabled   0          3600       256      256        disabled
```

Table 25-2 provides an explanation of the command output.

Table 25-2 show macauthentication Output Details

Output...	What it displays...
MAC authentication	Whether MAC authentication is globally enabled or disabled. Set using the **set macauthentication** command as described in "set macauthentication" on page 25-29.
MAC user password	User password associated with MAC authentication on the device. Set using the **set macauthentication password** command as described in "set macauthentication password" on page 25-29.
Port username significant bits	Number of significant bits in the MAC addresses to be used starting with the left-most bit of the vendor portion of the MAC address. The significant portion of the MAC address is sent as a user-name credential when the primary attempt to authenticate the full MAC address fails. Any other failure to authenticate the full address, (i.e., authentication server timeout) causes the next attempt to start once again with a full MAC authentication. Default is 48 and cannot be reset.

Downloaded from www.Manualslib.com manuals search engine

Table 25-2 show macauthentication Output Details (continued)

Output...	What it displays...
Port	Port designation. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.
Port State	Whether or not MAC authentication is enabled or disabled on this port.
Quiet Period	Enables a reauthentication attempt for failed entries at the period specified in seconds. Default value is 0 (never).
Reauth Period	Reauthentication period for this port. Default value of **30** can be changed using the **set macauthentication reauthperiod** command described in "set macauthentication reauthperiod" on page 25-35.
Auth Allowed	Number of concurrent authentications supported on this port. Default is 1 and cannot be reset.
Auth Allocated	Maximum number of MAC authentications permitted on this port. Default is 1 and cannot be reset.
Reauthentications	Whether or not reauthentication is enabled or disabled on this port. Set using the **set macauthentication reauthentication** command described in "set macauthentication reauthentication" on page 25-34.

show macauthentication session

Use this command to display the active MAC authenticated sessions.

Syntax

```
show macauthentication session
```

Parameters

None.

Defaults

If *port-string* is not specified, MAC session information will be displayed for all MAC authentication ports.

Mode

Switch command, Read-Only.

Example

This example shows how to display MAC session information:

```
Matrix(rw)->show macauthentication session
Port       MAC Address      Duration   Reauth Period   Reauthentications
-----    -----------------  ---------- -------------   -----------------
ge.1.2   00:60:97:b5:4c:07  0,00:52:31  3600           disabled
```

Table 25-3 provides an explanation of the command output.

Downloaded from www.Manualslib.com manuals search engine

Table 25-3 show macauthentication session Output Details

Output...	What it displays...
Port	Port designation. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.
MAC Address	MAC address associated with the session.
Duration	Time this session has been active.
Reauth Period	Reauthentication period for this port, set using the **set macauthentication reauthperiod** command described in "set macauthentication reauthperiod" on page 25-35.
Reauthentications	Whether or not reauthentication is enabled or disabled on this port. Set using the **set macauthentication reauthentication** command described in "set macauthentication reauthentication" on page 25-34.

set macauthentication

Use this command to globally enable or disable MAC authentication.

Syntax

set macauthentication {**enable** | **disable**}

Parameters

enable | **disable**	Globally enables or disables MAC authentication.

Defaults

Disabled.

Mode

Switch command, Read-Write.

Examples

This example shows how to globally enable MAC authentication:

```
Matrix(rw)->set macauthentication enable
```

set macauthentication password

Use this command to set a MAC authentication password.

Syntax

set macauthentication password *password*

Parameters

password	Specifies a text string MAC authentication password.

Downloaded from www.Manualslib.com manuals search engine

Defaults

None.

Mode

Switch command, Read-Write.

Examples

This example shows how to set the MAC authentication password to “macauth”:

```
Matrix(rw)->set macauthentication password macauth
```

clear macauthentication password

Use this command to clear the MAC authentication password.

Syntax

clear macauthentication password

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Write.

Examples

This example shows how to clear the MAC authentication password:

```
Matrix(rw)->clear macauthentication password
```

set macauthentication significant-bits

Use this command to set the number of significant bits of the MAC address to use for authentication.

Syntax

set macauthentication significant-bits *number*

Parameters

number	Specifies a number of significant bits.

Defaults

None.

Downloaded from www.Manualslib.com manuals search engine

Mode

Switch command, Read-Write.

Examples

This example shows how to set the MAC authentication significant bits to 24:

```
Matrix(rw)->set macauthentication significant-bits 24
```

clear macauthentication significant-bits

Use this command to clear the MAC authentication significant bits setting.

Syntax

clear macauthentication significant-bits

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to clear the MAC authentication significant bits setting:

```
Matrix(rw)->clear macauthentication significant-bits
```

set macauthentication port

Use this command to enable or disable one or more ports for MAC authentication.

Syntax

set macauthentication port {**enable** | **disable**} *port-string*

Parameters

enable | **disable**	Enables or disables MAC authentication.
port-string	Specifies port(s) on which to enable or disable MAC authentication. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.

Defaults

None.

Mode

Switch command, Read-Write.

Downloaded from www.Manualslib.com manuals search engine

Usage

Enabling port(s) for MAC authentication requires globally enabling MAC authentication on the device as described in "set macauthentication" on page 25-29, and then enabling it on a port-by-port basis. By default, MAC authentication is globally disabled and disabled on all ports.

Example

This example shows how to enable MAC authentication on ge.2.1 though 5:

```
Matrix(rw)->set macauthentication port enable ge.2.1-5
```

set macauthentication authallocated

Use this command to set the number of MAC authentication sessions allowed for one or more ports.

Syntax

set macauthentication authallocated *number port-string*

Parameters

number	Specifies the number of authentication sessions allowed.
port-string	Specifies port(s) on which to set the number of authentication sessions. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to set the number of allowed MAC authentication sessions to 4 on ge.2.1:

```
Matrix(rw)->set macauthentication authallocated 4 ge.2.1
```

clear macauthentication authallocated

Use this command to clear the number of MAC authentication sessions allowed for one or more ports.

Syntax

clear macauthentication authallocated [*port-string*]

Parameters

port-string	(Optional) Clears the number of authentication sessions allowed for specific port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.

Downloaded from www.Manualslib.com manuals search engine

Defaults

If *port-string* is not specified the number of allowed authentication sessions will be cleared on all ports.

Mode

Switch command, Read-Write.

Example

This example shows how to clear the number of allowed MAC authentication sessions on ge.2.1:

```
Matrix(rw)->clear macauthentication authallocated ge.2.1
```

set macauthentication portinitialize

Use this command to force one or more MAC authentication ports to re-initialize and remove any currently active sessions on those ports.

Syntax

set macauthentication portinitialize *port-string*

Parameters

port-string	Specifies the MAC authentication port(s) to re-initialize. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to force ge.2.1 through 5 to initialize:

```
Matrix(rw)->set macauthentication portinitialize ge.2.1-5
```

set macauthentication macinitialize

Use this command to force a current MAC authentication session to re-initialize and remove the session.

Syntax

set macauthentication macinitialize *mac_addr*

Parameters

mac_addr	Specifies the MAC address of the session to re-initialize.

Downloaded from www.Manualslib.com manuals search engine

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to force the MAC authentication session for address 00-60-97-b5-4c-07 to re-initialize:

```
Matrix(rw)->set macauthentication macinitialize 00-60-97-b5-4c-07
```

set macauthentication reauthentication

Use this command to enable or disable reauthentication of all currently authenticated MAC addresses on one or more ports.

Syntax

set macauthentication reauthentication {**enable** | **disable**} *port-string*

Parameters

enable | **disable**	Enables or disables MAC reauthentication.
port-string	Specifies port(s) on which to enable or disable MAC reauthentication. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to enable MAC reauthentication on ge.4.1 though 5:

```
Matrix(rw)->set macauthentication reauthentication enable ge.4.1-5
```

set macauthentication portreauthenticate

Use this command to force an immediate reauthentication of the currently active sessions on one or more MAC authentication ports.

Syntax

set macauthentication portreauthenticate *port-string*

Downloaded from www.Manualslib.com manuals search engine

Parameters

port-string	Specifies MAC authentication port(s) to be reauthenticated. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to force ge.2.1 though 5 to reauthenticate:

```
Matrix(rw)->set macauthentication portreauthentication ge.2.1-5
```

set macauthentication macreauthenticate

Use this command to force an immediate reauthentication of a MAC address.

Syntax

set macauthentication macreauthenticate *mac_addr*

Parameters

mac_addr	Specifies the MAC address of the session to reauthenticate.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to force the MAC authentication session for address 00-60-97-b5-4c-07 to reauthenticate:

```
Matrix(rw)->set macauthentication macreauthenticate 00-60-97-b5-4c-07
```

set macauthentication reauthperiod

Use this command to set the MAC reauthentication period (in seconds).

Syntax

set macauthentication reauthperiod *time port-string*

Downloaded from www.Manualslib.com manuals search engine

Parameters

time	Specifies the number of seconds between reauthentication attempts. Valid values are **1** - **4294967295**.
port-string	Specifies the port(s) on which to set the MAC reauthentication period. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.

Defaults

None.

Mode

Switch command, Read-Write.

Usage

This is the time lapse between attempts to reauthenticate any current MAC address authenticated to a port.

Example

This example shows how to set the MAC reauthentication period to 7200 seconds (2 hours) on ge.2.1 through 5:

```
Matrix(rw)->set macauthentication reauthperiod 7200 ge.2.1-5
```

clear macauthentication reauthperiod

Use this command to clear the MAC reauthentication period on one or more ports.

Syntax

clear macauthentication reauthperiod [*port-string*]

Parameters

port-string	(Optional) Clears the MAC reauthentication period on specific port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.

Defaults

If port-string is not specified, the reauthentication period will be cleared on all ports.

Mode

Switch command, Read-Write.

Example

This example shows how to globally clear the MAC reauthentication period:

```
Matrix(rw)->clear macauthentication reauthperiod
```


Downloaded from www.Manualslib.com manuals search engine

set macauthentication quietperiod

Use this command to enable a reauthentication attempt for failed entries at the period specified in seconds.

Syntax

set macauthentication quietperiod *time port-string*

Parameters

time	Specifies the number of seconds between reauthentication attempts. Valid values are **0** - **4294967295**.
port-string	Specifies the port(s) on which to set the macauthentication quiet period. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.

Defaults

None.

Mode

Switch command, Read-Write.

Usage

Default value is 0 (never).

Example

This example shows how to set the macauthentication quiet period to 120 seconds (2 minutes) on ge.2.1 through 5:

```
Matrix(rw)->set macauthentication quiet period 120 ge.2.1-5
```

clear macauthentication quietperiod

Use this command to clear the macauthentication quiet period on one or more ports to the default value.

Syntax

clear macauthentication quietperiod [*port-string*]

Parameters

port-string	(Optional) Clears the macauthentication quiet period on specific port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.

Defaults

None.

Mode

Switch command, Read-Write.

Downloaded from www.Manualslib.com manuals search engine

Usage

The default value is 0 (never).

Example

This example shows how to clear the macauthentication quietperiod for port ge.1.1

```
Matrix(rw)->clear macauthentication quietperiod ge.1.1:
```


Downloaded from www.Manualslib.com manuals search engine

Configuring Convergence End Points (CEP) Phone Detection

About CEP Phone Detection

Convergence is a method to detect a remote IP telephony or video device and apply a policy to the connection port based on the type of CEP device found. When a convergence end point (CEP) is found, the global policy for CEP detection is applied to the user on that port. The following phone detection types are available on Enterasys Matrix DFE devices:

- Cisco Phone Detection – Uses the Cisco Discovery Protocol (CiscoDP) to detect IP phones. When using Cisco phone detection, CiscoDP must be enabled and configured properly as described in "Cisco Discovery Protocol" on page 3-8.
- Siemens or Hipath Phone Detection – Uses either an IP address or a UDP / TCP port number for detection. By default UDP port 4060 will be used and there is no IP address configured. The commands in this section can be used to configure Siemens detection using new parameters.
- H.323 Phone Detection – Uses either a UDP / TCP port number with multicast group IP address or a UDP / TCP port number for detection. Default UDP ports are 1718,1719,1720. Default group address is 224.0.1.41. The commands in this section can be used to configure H.323 detection using new parameters. A second default H.323 detection excludes the default group address.
- SIP Phone Detection – Uses either a UDP / TCP port number with multicast group IP address or a UDP / TCP port number for detection. Default UDP / TCP port is 5060 and a multicast IP of 224.0.1.75. A second default SIP detection excludes the default group address.



Note: There is no way to detect if a Siemens, SIP or H.323 phone goes away other than a link down. Therefore, if these types of phones are not directly connected to the switch's port and the phone goes away, the switch will still think there is a phone connection and any configured policy will remain on the port. Detected CEPs will be removed from the connection table if they do not send traffic for a period of time equal to the etsysMultiAuthIdleTimeout value. Additionally, CEPs will be removed if the total duration of their sessions exceeds the time specified by etsysMultiAuthSessionTimeout.

Purpose

To review, set the status and configure CEP phone detection.

Commands

For information about...	Refer to page...
show cep connections	25-40
show cep detection	25-40
show cep policy	25-41
show cep port	25-42
set cep	25-42
set cep port	25-43
set cep policy	25-43
set cep detection-id	25-44

Downloaded from www.Manualslib.com manuals search engine

For information about...	Refer to page...
set cep detection-id type	25-45
set cep detection-id address	25-46
set cep detection-id protocol	25-46
set cep detection-id porthigh | portlow	25-47
set cep initialize	25-48
clear cep	25-49

show cep connections

Use this command to display all learned CEPs.

Syntax

show cep connections *port-string*

Parameters

port-string	Displays CEP status for one or more ports. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.

Defaults

None

Mode

Read-Only.

Example

This example shows how to display CEP connections for port fe.1.21:

```
Matrix>show cep connections fe.1.21
Connection Info for fe.1.21
Endpoint Type      h323
Policy Index       3
Discovery Time     MON FEB 06 02:31:42 2006
Firmware Version
Address Type       unknown
Endpoint IP        unavailable
Endpoint MAC       00:04:0d:01:f8:35
```

show cep detection

Use this command to display CEP phone detection parameters.

Syntax

show cep detection [*detection-id*]

Downloaded from www.Manualslib.com manuals search engine

Parameters

detection-id	(Optional) Show CEP detection parameters, based on the CEP configuration group id.

Defaults

If no *detection-id* is specified, all CEP detection parameters are displayed.

Mode

Read-Only.

Examples

This example shows how to display CEP detection information:

```
Matrix>show cep detection
Global CEP state enabled
Detection Rules for Index 1:
Endpoint Phone Type h323
Protocol tcp & udp
Port Low 1718
Port High 1720
Address Type unknown
Address
Mask Type unknown
Mask
Row Status enabled
```

show cep policy

Use this command to display the global policies of all supported CEP types.

Syntax

show cep policy

Parameters

None.

Defaults

None

Mode

Read-Only.

Downloaded from www.Manualslib.com manuals search engine

Examples

This example shows how to display CEP policy information:

```
Matrix>show cep policy
CEP default policies
CEP Type  Policy Index  Policy Name
--------  ------------  ------------
cisco     13            Cisco IP Phone
siemens   9             IP Phone Siemens
h323      3             IP Phone Avaya
sip       0
```

show cep port

Use this command to display enable status of all supported CEP types.

Syntax

show cep port *port-string*

Parameters

port-string	Displays CEP status for one or more ports. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.

Defaults

None

Mode

Read-Only.

Examples

This example shows how to display CEP status information for port fe.1.21:

```
Matrix>show cep port fe.1.21
Port          H323     Siemens    Cisco     SIP
----------  --------  --------  --------  --------
fe.1.21     enabled   enabled   enabled   disabled
```

set cep

Use this command to globally enable or disable CEP detection.

Syntax

set cep {**enable** | **disable**}

Parameters

enable | **disable**	Globally enables or disables CEP detection.

Downloaded from www.Manualslib.com manuals search engine

Defaults

Disabled.

Mode

Switch command, Read-Write.

Example

This example shows how to globally enable CEP detection:

```
Matrix>set cep enable
```

set cep port

Use this command to enable or disable a CEP detection type on one or more ports.

Syntax

set cep port *port-string* {**cisco** | **h323** | **lldp-med** | **siemens** | **sip**} {**enable** | **disable**}

Parameters

port-string	Specifies the port(s) to enable or disable. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.
cisco	Set the Cisco detection status on the specified ports.
h323	Set the H323 detection status on the specified ports.
lldp-med	Set the LLDP-MED detection status on the specified ports.
siemens	Set the Siemens detection status on the specified ports.
sip	Set the SIP detection status on the specified ports.
enable | **disable**	Enables or disables CEP detection as specified.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to enable Cisco phone detection on port fe. 3. 1:

```
Matrix>set cep port fe.3.1 cisco enable
```

set cep policy

Use this command to set a global default policy for a CEP detection type.

Syntax

set cep policy {**cisco** | **h323** | **siemens** | **sip**} *index*

Downloaded from www.Manualslib.com manuals search engine

Parameters

cisco	Set the Cisco global default policy index.
h323	Set the H323global default policy index.
siemens	Set the Siemens global default policy index.
sip	Set the SIP global default policy index.
index	Set the policy index value. This must be configured using the policy management commands described in Chapter 8. Valid values are **1** - **65535**.

Defaults

None.

Mode

Switch command, Read-Write.

Usage

This is the policy that will be applied when a phone of the specified type is detected on a port. It must be configured using the policy management commands described in Chapter 8.

Example

This example shows how to assign policy index 1:

```
Matrix>set cep policy h323 1 to all H.323 phones detected
```

set cep detection-id

Use this command to create a new H.323, Siemens, or SIP phone detection configuration group, or enable, disable or remove an existing group.

Syntax

set cep detection-id *id* {**create** | **delete** | **disable** | **enable**}

Parameters

id	Specifies a CEP configuration group value. Valid values are **1** - **2147483647**.
create | **delete** | **disable** | **enable**	Creates a new convergence end points detection configuration group, or removes, disables or enables an existing group. A group must first be created then enabled to become operational.

Defaults

None.

Mode

Switch command, Read-Write.

Downloaded from www.Manualslib.com manuals search engine

Usage

This command applies only to Siemens, H.323, and SIP phone detection. Cisco detection uses CiscoDP as its discovery method.

Example

This example shows how to create CEP detection group 1:

```
Matrix>set cep detection-id 1 create
```

set cep detection-id type

Use this command to specify whether a phone detection group will use H.323, Siemens or SIP as its phone discovery type.

Syntax

set cep detection-id *id* **type** {**h323** | **siemens** | **sip**}

Parameters

id	Specifies a CEP configuration group ID. This group must be created and enabled using the **set cep detection-id** command as described in "set cep detection-id" on page 25-44. Valid values are **1** - **2147483647**.
h323 | siemens | sip	Specifies the phone type to detect as H.323,Siemens or SIP.

Defaults

None.

Mode

Switch command, Read-Write.

Usage

This command applies only to Siemens, H.323, and SIP phone detection. Cisco detection uses CiscoDP as its discovery method.

There are currently 3 manual detection types (Siemens, H323, SIP). Under manual detection configuration, for each of the types, the "Endpoint Phone Type" will be listed correctly. However, the high and low ports will not reflect default ports for the "Endpoint Phone Types". The user will have to configure the port low and high options to match their needs for the Endpoint Phone Type being configured, as described in "set cep detection-id porthigh | portlow" on page 25-47.

Example

This example shows how to set the phone detection type to H.323 for CEP group 1:

```
Matrix>set cep detection-id 1 type h323
```


Downloaded from www.Manualslib.com manuals search engine

set cep detection-id address

Use this command to set an H.323, Siemens, or SIP phone detection group's IP address or mask.

Syntax

```
set cep detection-id id address { ip-address | unknown }
mask {mask | unknown }
```

Parameters

id	Specifies a CEP configuration group ID. This group must be created and enabled using the **set cep detection-id** command as described in "set cep detection-id" on page 25-44. Valid values are **1** - **2147483647**.
address *ip-address* | **unknown**	Sets the IP address for CEP detection, or sets the address to **unknown**.
mask *mask* | **unknown**	Set the IP mask for CEP detection, or sets the mask to **unknown**.

Defaults

None.

Mode

Switch command, Read-Write.

Usage

This command applies only to Siemens, H.323, and SIP phone detection. Cisco detection uses CiscoDP as its discovery method.

By default, H.323 will use 224.0.1.41 as its IP address and Siemens will have no IP address configured.

Example

This example shows how to set an IP address of 10.1.1.3 and mask for detection group 1:

```
Matrix>set cep detection-id 1 address 10.1.1.3 mask 255.255.0.0
```

set cep detection-id protocol

Use this command to specify an IP protocol type for H.323, Siemens, or SIP convergence end points detection.

Syntax

```
set cep detection-id id protocol {tcp | udp | both | none}
```


Downloaded from www.Manualslib.com manuals search engine

Parameters

id	Specifies a CEP configuration group ID. This group must be created and enabled using the **set cep detection-id** command as described in "set cep detection-id" on page 25-44. Valid values are **1** - **2147483647**.
tcp | **udp** | **both** | **none**	Sets the CEP IP protocol type to be used for detection as: • TCP • UDP • Both UDP and TCP • None

Defaults

None.

Mode

Switch command, Read-Write.

Usage

This command applies only to Siemens, H.323, and SIP phone detection. Cisco detection uses CiscoDP as its discovery method.

If an IP address is not set for a phone detection group as described in "set cep detection-id address" on page 25-46, this will configure detection on UDP and/or TCP ports using a port range defined with the **set cep detection-id porthigh** | **portlow** command as described in "set cep detection-id porthigh | portlow" on page 25-47.

Example

This example shows how to enable both TCP and UDP convergence end points detection for CEP detection group 1:

```
Matrix>set cep detection-id 1 protocol both
```

set cep detection-id porthigh | portlow

Use this command to set the maximum and minimum ports used for TCP or UDP convergence end points detection.

Syntax

set cep detection-id *id* { **porthigh** | **portlow** } *port*

Parameters

id	Specifies a CEP configuration group ID. This group must be created and enabled using the **set cep detection-id** command as described in "set cep detection-id" on page 25-44. Valid values are **1** - **2147483647**.
porthigh | **portlow** *port*	Specifies a maximum or minimum UDP or TCP port for CEP detection.Valid values are **1** - **65535**.

Defaults

None.

Downloaded from www.Manualslib.com manuals search engine

Mode

Switch command, Read-Write.

Usage

This command applies only to Siemens, H.323, and SIP phone detection. Cisco detection uses CiscoDP as its discovery method.

Once UDP and/or TCP phone detection has been specified using the **set cep detection-id protocol** command as described in "set cep detection-id protocol" on page 25-46, the protocols will use this port range for detection matching.

Example

This example shows how to set port 65 as the minimum port to be used for convergence end points detection for CEP group 1:

```
Matrix>set cep detection-id 1 portlow 65
```

set cep initialize

Use this command to clear all existing CEP connections for one or more CEP-enabled ports.

Syntax

set cep initialize [*port-string*]

Parameters

port-string	(Optional) Specifies the CEP-enabled port(s) to clear existing CEP connections. This must be a *port-string* enabled for CEP using the **set cep port** command as described in "set cep port" on page 25-43. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.

Defaults

If no *port-string* is specified, all existing CEP connections on all ports are cleared.

Mode

Switch command, Read-Write.

Usage

This command is similar to the **clear cep users** command.

Example

This example shows how to re-initialize CEP ports fe.1.3-5:

```
Matrix>set cep initialize fe.1.3-5
```


Downloaded from www.Manualslib.com manuals search engine

clear cep

Use this command to clear convergence end points parameters.

Syntax

clear cep {**all** | **policy** | **detection** [*detection-id*] | **users** [*port-string*] | **port** [*port-string* {**all** | **cisco** | **h323** | **siemens** |**sip**}] }

Parameters

all	Restores factory defaults to all CEP configuration information.
policy	Restore factory defaults to CEP policy configuration.
detection [*detection-id*]	Restore factory defaults to CEP detection group configuration. Optionally, specify a particular CEP configuration group to clear with *detection-id*. Valid values are **1** - **2147483647**.
users [*port-string*]	Clear discovered Convergence Endpoints. Optionally, specify one or more port(s) on which to clear discovered CEPs. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.
port [*port-string* {**all** | **cisco** | **h323** | **siemens** | **sip** }]	Resets the CEP enabled state to the default of disabled. Optionally, specify one or more port(s) to disable and specify all detection types or individual detection types to disable. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 4-2.

Defaults

If no *detection-id* is specified, all CEP detection groups are returned to the default configuration.

If no *port-string* is specified with the **users** parameter, all discovered Convergence Endpoints are cleared.

If no *port-string* is specified with the port parameter, all ports are cleared.

Mode

Switch command, Read-Write.

Examples

This example shows how to clear all CEP policy parameters

```
Matrix>clear cep policy
```

This example shows how to clear detection id 4 parameters

```
Matrix>clear cep detection-id 4
```

This example shows how to clears ports fe.1.1-5 of Cisco phone detection parameters

```
Matrix>clear cep port fe.1.1-5 cisco
```


Downloaded from www.Manualslib.com manuals search engine

RADIUS Filter-ID Attribute and Dynamic Policy Profile Assignment

If you configure an authentication method that requires communication with a RADIUS server, you can use the RADIUS Filter-ID attribute to dynamically assign a policy profile and/or management level to authenticating users and/or devices.

The RADIUS Filter-ID attribute is simply a string that is formatted in the RADIUS Access-Accept packet sent back from the RADIUS server to the switch during the authentication process.

Each user can be configured in the RADIUS server database with a RADIUS Filter-ID attribute that specifies the name of the policy profile and/or management level the user should be assigned upon successful authentication. During the authentication process, when the RADIUS server returns a RADIUS Access-Accept message that includes a Filter-ID matching a policy profile name configured on the switch, the switch then dynamically applies the policy profile to the physical port the user/device is authenticating on.

Filter-ID Attribute Formats

Enterasys Networks supports two Filter-ID formats — "decorated" and "undecorated." The decorated format has three forms:

- To specify the policy profile to assign to the authenticating user (network access authentication):

  Enterasys:version=1:policy=*string*

  where *string* specifies the policy profile name. Policy profile names are case-sensitive.

- To specify a management level (management access authentication):

  Enterasys:version=1:mgmt=*level*

  where *level* indicates the management level, either **ro**, **rw**, or **su**.

- To specify both management level and policy profile:

  Enterasys:version=1:mgmt=*level*:policy=*string*

The undecorated format is simply a string that specifies a policy profile name. The undecorated format cannot be used for management access authentication.

Decorated Filter-IDs are processed first. If no decorated Filter-IDs are found, then undecorated Filter-IDs are processed. If multiple Filter-IDs are found that contain conflicting values, a Syslog message is generated.

Setting the Authentication Login Method

Purpose

To configure the authentication login method.

Commands

The commands used to configure the authentication login method are listed below and described in the associated section as shown:

Downloaded from www.Manualslib.com manuals search engine

For information about...	Refer to page...
show authentication login	25-51
set authentication login	25-51
clear authentication login	25-52

show authentication login

Use this command to display the current authentication login method.

Syntax

```
show authentication login
```

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Only.

Example

This example shows how to display the current authentication login method:

```
Matrix(rw)->show authentication login
Current authentication login is any
```

set authentication login

Use this command to set the authentication login method.

Syntax

```
set authentication login {any | local | radius | tacacs}
```

Parameters

any	Specifies that the authentication protocol will be selected using the following precedence order: • TACACS+ • RADIUS • Local
local	Specifies that the local network password settings will be used for authentication login.
radius	Specifies that RADIUS will be used for authentication login.
tacacs	Specifies that TACACS+ will be used for authentication login.

Downloaded from www.Manualslib.com manuals search engine

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to set the authentication login method to use the local password settings:

```
Matrix(rw)->set authentication login local
```

clear authentication login

Use this command to reset the authentication login method to the default setting of “any”.

Syntax

clear authentication login

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to reset the authentication login method:

```
Matrix(rw)->clear authentication login
```


Downloaded from www.Manualslib.com manuals search engine

Configuring RADIUS

Purpose

To perform the following:

- Review the RADIUS client/server configuration on the device.
- Enable or disable the RADIUS client.
- Set local and remote login options.
- Set primary and secondary server parameters, including IP address, timeout period, authentication realm, and number of user login attempts allowed.
- Reset RADIUS server settings to default values.
- Configure a RADIUS accounting server.

Commands

For information about...	Refer to page...
show radius	25-53
set radius	25-54
clear radius	25-55
show radius accounting	25-56
set radius accounting	25-57
clear radius accounting	25-58

show radius

Use this command to display the current RADIUS client/server configuration.

Syntax

show radius [**state** | **retries authtype** || **timeout** | **server** [*index* | **all**]]

Parameters

state	(Optional) Displays the RADIUS client's enable status.
retries	(Optional) Displays the number of retry attempts before the RADIUS server times out.
authtype	(Optional) Displays the RADIUS server's authentication type.
server	(Optional) Displays RADIUS server configuration information.
timeout	(Optional) Displays the maximum amount of time (in seconds) to establish contact with the RADIUS server before retry attempts begin.
index | **all**	(Optional) Displays configuration information for a specified server or all RADIUS servers.

Downloaded from www.Manualslib.com manuals search engine

Defaults

If no parameters are specified, all RADIUS configuration information will be displayed.

Mode

Switch command, Read-Only.

Example

This example shows how to display RADIUS configuration information:

```
Matrix(rw)->show radius
RADIUS state:       Enabled
RADIUS retries:     2
RADIUS timeout:     3 seconds
RADIUS Server    IP Address       Auth-Port  Realm-Type          Status --------
-- --------------- ---------  ------------------       -------
1                 100.10.0.100     1812       any                 Active
```

Table 25-4 provides an explanation of the command output.

Table 25-4 show radius Output Details

Output...	What it displays...
RADIUS state	Whether the RADIUS client is **enabled** or **disabled**.
RADIUS retries	Number of retry attempts before the RADIUS server times out. The default value of **3** can be reset using the **set radius** command as described in “set radius” on page 25-54.
RADIUS timeout	Maximum amount of time (in seconds) to establish contact with the RADIUS server before retry attempts begin. The default value of **20** can be reset using the **set radius** command as described in “set radius” on page 25-54.
RADIUS Server	IP address, UDP authentication port, authentication realm type (**management**, **network** or **any**), and status (whether or not the RADIUS server has been configured).

set radius

Use this command to enable, disable, or configure RADIUS authentication.

Syntax

set radius {[**enable** | **disable**] [**retries** *number-of-retries*] [**timeout** *timeout*] [**server** {*index ip-address port* [*secret-value*]} [**realm** {**management-access** | **network-access** | **any**} {*index* | **all**}]}

Parameters

enable | **disable**	Enables or disables the RADIUS client.
retries *number-of-retries*	Specifies the number of retry attempts before the RADIUS server times out. Valid values are from **1** to **10**. Default is **3**.

Downloaded from www.Manualslib.com manuals search engine

timeout *timeout*	Specifies the maximum amount of time (in seconds) to establish contact with the RADIUS server before retry attempts begin. Valid values are from **1** to **30**. Default is **20** seconds.
server *index ip_address port*	Specifies the index number, IP address and the UDP authentication port for the RADIUS server.
secret-value	(Optional) Specifies an encryption key to be used for authentication between the RADIUS client and server.
realm management -access | **network-access** | **any**	(Optional) Restricts the RADIUS server realm to management or network access authentication, or allows it to perform all authentications.
index | **all**	Applies the server realm setting to a specific server or to all servers.

Defaults

- If *secret-value* is not specified, none will be applied.
- If **realm** is not specified, **any** authentication will be allowed.

Mode

Switch command, Read-Write.

Usage

The RADIUS client can only be enabled on the switch once a RADIUS server is online, and its IP address(es) has been configured with the same password the RADIUS client will use.

Examples

This example shows how to enable the RADIUS client for authenticating with RADIUS server 1 at IP address 10.1.6.203, UDP authentication port 1812, and an authentication password of "pwsecret." As previously noted, the "server secret" password entered here must match that already configured as the Read-Write (rw) password on the RADIUS server:

```
Matrix(rw)->set radius server 1 10.1.6.203 1812 pwsecret
```

This example shows how to restrict all RADIUS servers to authenticate management access only

```
Matrix(rw)->set radius realm management-access all
```

This example shows how to set the RADIUS timeout to 5 seconds:

```
Matrix(rw)->set radius timeout 5
```

This example shows how to set RADIUS retries to 10:

```
Matrix(rw)->set radius retries 10
```

clear radius

Use this command to clear RADIUS server settings.

Syntax

clear radius [**state**] [**retries**] [**timeout**] [**server** [*index* | **all**] [**realm** {*index* | **all**}]

Downloaded from www.Manualslib.com manuals search engine

Parameters

state	(Optional) Resets the RADIUS client state to the default setting of disabled.
retries	(Optional) Resets the maximum number of attempts a user can contact the RADIUS server before timing out to **3**.
timeout	(Optional) Resets the maximum amount of time to establish contact with the RADIUS server before timing out to **20** seconds.
server	(Optional) Deletes server settings.
realm	(Optional) Resets the realm setting to allowing any authentication.
index | **all**	Resets settings for a specified server or all RADIUS servers.

Defaults

- If *index* or **all** is not specified for clearing RADIUS server, all RADIUS server settings will be deleted.
- If no other optional parameters are specified, all RADIUS settings will be cleared.

Mode

Switch command, Read-Write.

Examples

This example shows how to clear all settings on all RADIUS servers:

```
Matrix(rw)->clear radius server all
```

This example shows how to reset the RADIUS timeout to the default value of 20 seconds:

```
Matrix(rw)->clear radius timeout
```

show radius accounting

Use this command to display the RADIUS accounting configuration. This transmits accounting information between a network access server and a shared accounting server.

Syntax

show radius accounting [**updateinterval**] | [**intervalminimum**] | [**state**] | [**server** {*index* | **all**}]

Parameters

updateinterval	(Optional) Displays the number of seconds between each RADIUS accounting interim update (when accumulated accounting data is sent to the server for a session.)
intervalminimum	(Optional) Displays the minimum update interval setting. This controls the frequency of RADIUS accounting updates.
state	(Optional) Displays the RADIUS accounting enable state.
server *index* | **all**	(Optional) Displays one or all RADIUS accounting server configurations.

Downloaded from www.Manualslib.com manuals search engine

Defaults

If no parameters are specified, all RADIUS accounting configuration information will be displayed.

Mode

Switch command, Read-Only.

Example

This example shows how to display RADIUS accounting configuration information. In this case, RADIUS accounting is enabled and global default settings have not been changed. One server has been configured. The Enterasys Matrix Series device allows for up to 10 RADIUS accounting servers to be configured, with up to 2 active at any given time.

For details on enabling and configuring RADIUS accounting, refer to "set radius accounting" on page 25-57:

```
Matrix(rw)->show radius accounting
Accounting state:              Enabled
Accounting update interval:    1800 secs
Accounting interval minimum:   600 secs

Server        Server          Acct
Index           IP            Port  Retries  Timeout     Status
-------------------------------------------------------------------
1           1.1.1.1           1236     2        5        Primary
```

set radius accounting

Use this command to configure RADIUS accounting.

Syntax

set radius accounting {[**enable**] [**disable**] [**intervalminimum** *value*] [**updateinterval** *value*] [**retries** *retries*] [**timeout** *timeout*] [**server** {*index* | **all**} *ip_address port* [*server-secret*]

Parameters

enable | **disable**	Enables or disables the RADIUS accounting client.
intervalminimum *value*	Sets the minimum interval at which RADIUS accounting will send interim updates. Valid values are **60** - **2147483647**.
updateinterval *value*	Sets the number of seconds between each RADIUS accounting interim update (when accumulated accounting data is sent to the server for a session.) Valid values are **180** - **2147483647**.
retries *retries*	Sets the maximum number of attempts to contact a specified RADIUS accounting server before timing out. Valid retry values are **1** - **2147483647**.
timeout *timeout*	Sets the maximum amount of time (in seconds) to establish contact with a specified RADIUS accounting server before timing out. Valid timeout values are **1** - **2147483647**.

Downloaded from www.Manualslib.com manuals search engine

index | **all**	Applies the settings to a specific RADIUS accounting server or to all.
server *ip_address* port server-secret	Specifies the accounting server's: • IP address • UDP authentication port (**0** - **65535)** • *server-secret* (Read-Write password to access this accounting server. Device will prompt for this entry upon creating a server instance, as shown in the example below.)

Defaults

None.

Mode

Switch command, Read-Write.

Examples

This example shows how to enable the RADIUS accounting client for authenticating with the accounting server 1 at IP address 10.2.4.12, UDP authentication port 1800. As previously noted, the "server secret" password entered here must match that already configured as the Read-Write (rw) password on the RADIUS accounting server

```
Matrix(rw)->set radius accounting server 1 10.2.4.12 1800:
 Server Secret:******
 Retype Server Secret:******
 Make This Entry Active (y/n)? y
 Warning: rfc2138 recommends secret minimum length of 16
```

This example shows how to set the RADIUS accounting timeout to 30 seconds on server 6:

```
Matrix(rw)->set radius accounting timeout 30 6
```

This example shows how to set RADIUS accounting retries to 10 on server 6:

```
Matrix(rw)->set radius accounting retries 10 6
```

clear radius accounting

Use this command to clear RADIUS accounting configuration settings.

Syntax

clear radius accounting {[**server**{*index* | **all**}] [**retries** {*index* | **all**}] [**timeout** {*index* | **all**}] [**intervalminimum**] [**updateinterval**]}

Parameters

server *index* | **all**	Clears the configuration on one or more accounting servers.
retries *index* | **all**	Resets the retries to the default value of 2 on one or more accounting servers.
timeout *index* | **all**	Resets the timeout to 5 seconds on one or more accounting servers.
intervalminimum	Resets the minimum interval to 600 seconds.
updateinterval	Resets the update interval to 1800 seconds.

Downloaded from www.Manualslib.com manuals search engine

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to reset the RADIUS accounting timeout to 5 seconds on all servers:

```
Matrix(rw)->clear radius accounting timeout all
```


Downloaded from www.Manualslib.com manuals search engine

Configuring RFC 3580

About RFC 3580

RFC 3580 provides suggestions on how 802.1x Authenticators should leverage RADIUS as the backend AAA infrastructure. RFC 3580 is divided into several major sections: RADIUS Accounting, RADIUS Authentication, RC4 EAPOL-Key-Frame Discussions, and Security Considerations. Upon detection, End-Points (PCs, IP Phones, etc.) may be interrogated by the AAA clients for credentials, which may then be used to authenticate the user and determine the services which should be provided (authorization). During the exchange with the AAA server, the AAA client will present information describing the End-Point and itself. The AAA server will then describe the level of service which should be provided. This may include authentication success, session duration, and class-of-service to be provided.

Enterasys Networks Layer 2 switches utilize two specific attributes to implement the provisioning of service in response to a successful authentication:

- A proprietary Filter-ID, which describes a Policy Profile to be applied to the user. (See "RADIUS Filter-ID Attribute and Dynamic Policy Profile Assignment" on page 25-50.)
- The VLAN-Tunnel-Attribute; which defines the base VLAN-ID to be applied to the user (or possibly mapped to an Enterasys Policy Profile).

Purpose

To review and configure RFC 3580 support.

Commands

For information about...	Refer to page...
show vlanauthorization	25-60
set vlanauthorization	25-61
clear vlanauthorization	25-62

show vlanauthorization

Use this command to display the VLAN Authorization settings.

Syntax

show vlanauthorization [*port-list*] | [**all**]

Parameters

port-list	(Optional) Displays the port(s) VLAN Authorization settings.
all	(Optional) Displays all port(s) VLAN Authorization settings.

Defaults

If no parameters are specified, all VLAN Authorization configuration information will be displayed.

Downloaded from www.Manualslib.com manuals search engine

Mode

Switch command, Read-Only.

Example

This example shows how to display VLAN Authorization configuration information for ports ge.1.1-3:

```
Matrix(su)->show vlanauthorization ge.1.1-3
 VLAN Authorization Global Status:  enabled
 VLAN Authorization Table   :

 Port       Status       Admin Egress   Oper Egress    VLAN ID
-------------------------------------------------------------
 ge.1.1     enabled      untagged       untagged       4094
 ge.1.2     disabled     untagged       untagged       none
 ge.1.3     enabled      untagged       untagged       unknown
```

set vlanauthorization

Use this command to set the VLAN Authorization attributes.

Syntax

set vlanauthorization enable | **disable** | **port** *port-list* {[**enable** | **disable**] **none** | **tagged** | **untagged** | **dynamic**}

Parameters

enable | disable	**enable** - Enable VLAN Authorization. **disable** - Disable VLAN Authorization.
port *port-list*	(Optional) Set port(s) attributes for VLAN Authorization.
enable | disable	**enable** - Enable port VLAN Authorization. **disable** - Disable port VLAN Authorization.
none | tagged | untagged | dynamic	**none** - No egress change will be made. **tagged** - Port added to egress. **untagged** - Port added to untagged egress. **dynamic** - Use information in authentication response.

Defaults

None.

Mode

Switch command, Read-Write.

Downloaded from www.Manualslib.com manuals search engine

Example

This example shows how to enable VLAN Authorization:

```
Matrix(su)->set vlanauthorization enable
```

This example shows how to enable VLAN Authorization for port ge.1.1 for tagged packets:

```
Matrix(su)->set vlanauthorization port ge.1.1 enable tagged
```

clear vlanauthorization

Use this command to clear the VLAN Authorization attributes to the defaults.

Syntax

clear vlanauthorization *port-list* **all**

Parameters

port-list	(Optional) Clear port(s) attributes for VLAN Authorization.
all	Clear all VLAN Authorization to the defaults.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to clear VLAN Authorization:

```
Matrix(su)->clear vlanauthorization
```

This example shows how to clear VLAN Authorization for ports ge.1.1-4:

```
Matrix(su)->clear vlanauthorization ge.1.1-4
```


Downloaded from www.Manualslib.com manuals search engine

Configuring TACACS+

Purpose

To perform the following:

- Review the TACACS+ client and server configurations on the device.
- Enable or disable the TACACS+ client.
- Set local and remote login options.
- Set server parameters, including IP address, timeout period, server port, and secret.
- Reset TACACS+ client and server settings to default values.

Commands

For information about...	Refer to page...
show tacacs	25-63
set tacacs	25-65
show tacacs server	25-65
set tacacs server	25-66
clear tacacs server	25-67
show tacacs session	25-67
set tacacs session	25-68
clear tacacs session	25-69
show tacacs command	25-70
set tacacs command	25-71
show tacacs singleconnect	25-71
set tacacs singleconnect	25-72

show tacacs

Use this command to display the current TACACS+ configuration information and status.

Syntax

```
show tacacs [state]
```

Parameters

state	(Optional) Displays only the TACACS+ client status.

Defaults

If **state** is not specified, all TACACS+ configuration information will be displayed.

Downloaded from www.Manualslib.com manuals search engine

Mode

Switch command, Read-Only.

Example

This example shows how to display all TACACS configuration information:

```
Matrix(ro)->show tacacs
 TACACS+ state:                          enabled
 TACACS+ session accounting state:       disabled
 TACACS+ command authorization state:    disabled
 TACACS+ command accounting state:       disabled
 TACACS+ single-connect state:           disabled
 TACACS+ service:                        exec
 TACACS+ session authorization A-V pairs:
         access level attribute                          value
         read-only   'priv-lvl'                          '0'
         read-write  'priv-lvl'                          '1'
         super-user  'priv-lvl'                          '15'
 TACACS+ Server  IP Address       Port   Timeout  Status
 --------------  ---------------  -----  -------  -------
   1               10.1.26.245     49       10     Active
```

Table 25-5 provides an explanation of the command output.

Table 25-5 show tacacs Output Details

Output...	What it displays...
TACACS+ state	Whether the TACACS+ client is **enabled** or **disabled**.
TACACS+ session accounting state	Whether TACACS+ session accounting is **enabled** or **disabled**.
TACACS+ command authorization state	Whether TACACS+ command authorization is **enabled** or **disabled**.
TACACS+ command accounting state	Whether TACACS+ command accounting is **enabled** or **disabled**.
TACACS+ singleconnect state	Whether TACACS+ singleconnect is **enabled** or **disabled**. When enabled, the TACACS+ client sends multiple requests over a single TCP connection.
TACACS+ service	The name of the service that is requested by the TACACS+ client for session authorization. “exec” is the default service name.
TACACS+ session authorization A-V pairs	Displays the attribute – value pairs that are mapped to the Matrix **read-only**, **read-write**, and **super-user** access privilege levels for the service requested for session authorization. The attribute names and values shown in the example above are the default values.
TACACS+ Server	Displays the TACACS+ server information used by the TACACS+ client.

Downloaded from www.Manualslib.com manuals search engine

set tacacs

Use this command to enable or disable the TACACS+ client.

Syntax

```
set tacacs {enable | disable}
```

Parameters

enable | **disable**	Enables or disables the TACACS client.

Defaults

None.

Mode

Switch command, Read-Write.

Usage

The TACACS+ client can be enabled on the switch anytime, with or without a TACACS+ server online. If the TACACS+ server is offline and TACACS+ is enabled, the login authentication is switched to RADIUS or local, if enabled.

Examples

This example shows how to enable the TACACS+ client.

```
Matrix(rw)->set tacacs enable
```

show tacacs server

Use this command to display the current TACACS+ server configuration.

Syntax

```
show tacacs server {index | all}
```

Parameters

index	Display the configuration of the TACACS+ server identified by *index*. The value of *index* can range from 1 to 2,147,483,647.
all	Display the configuration for all configured TACACS+ servers.

Defaults

None.

Mode

Switch command, Read-Only.

Downloaded from www.Manualslib.com manuals search engine

Example

This example displays configuration information for all configured TACACS+ servers.

```
Matrix(ro)->show tacacs server all
 TACACS+ Server  IP Address       Port   Timeout  Status
 --------------  ---------------  -----  -------  -------
 1               192.168.10.10    49     10       Active
 2               192.168.1.116    49     10       Active
```

set tacacs server

Use this command to configure the TACACS+ server(s) to be used by the TACACS+ client. You can configure the timeout value for all configured servers or a single server, or you can configure the IP address, TCP port, and secret for a single server. For simplicity, two syntax statements are shown.

Syntax

set tacacs server {**all** | *index*} **timeout** *seconds*

set tacacs server *index address port secret*

Parameters

all	Specify the timeout value for all configured TACACS+ servers.
index	Configure the TACACS+ server identified by *index*. The value of *index* can range from 1 to 2,147,483,647.
timeout *seconds*	Set the timeout value for the specified server(s) in seconds. The value of *seconds* can range from 1 to 180 seconds. The default timeout value is 10 seconds.
address	Specify the IP address of the TACACS+ server.
port	Specify the TCP port for the TACACS+ server. The value of *port* can range from 0 to 65535, but typically, port 49 is specified.
secret	Specify the secret for the TACACS+ server.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example configures TACACS+ server 1. The default timeout value of 10 seconds will be applied.

```
Matrix(rw)->set tacacs server 1 192.168.10.10 49 mysecret
```


Downloaded from www.Manualslib.com manuals search engine

clear tacacs server

Use this command to remove one or all configured TACACS+ servers, or to return the timeout value to its default value for one or all configured TACACS+ servers.

Syntax

clear tacacs server {**all** | *index*} [**timeout**]

Parameters

all	Specifies that all configured TACACS+ servers should be affected.
index	Specifies one TACACS+ server to be affected.
timeout	(Optional) Return the timeout value to its default value of 10 seconds.

Defaults

If **timeout** is not specified, the affected TACACS+ servers will be removed.

Mode

Switch command, Read-Write.

Example

This example removes TACACS+ server 1.

```
Matrix(rw)->clear tacacs server 1
```

show tacacs session

Use this command to display the current TACACS+ client session settings.

Syntax

show tacacs session {**authorization** | **accounting** [**state**]}

Parameters

authorization	Display client session authorization settings.
accounting	Display client session accounting settings.
state	(Optional) Display the client session accounting state.

Defaults

If **state** is not specified, all session accounting configuration parameters are displayed (which at this time includes only the enabled/disabled status).

Mode

Switch command, Read-Only.

Examples

This example shows how to display client session authorization information:

Downloaded from www.Manualslib.com manuals search engine

```
Matrix(ro)->show tacacs session authorization
 TACACS+ service:                      exec
 TACACS+ session authorization A-V pairs:
         access level attribute                          value
         read-only   'priv-lvl'                          '0'
         read-write  'priv-lvl'                          '1'
         super-user  'priv-lvl'                          '15'
```

This example shows how to display client session accounting state.

```
Matrix(ro)->show tacacs session accounting state
 TACACS+ session accounting state:     enabled
```

set tacacs session

Use this command to enable or disable TACACS+ session accounting, or to configure TACACS+ session authorization parameters. For simplicity, separate syntax formats are shown for configuring session accounting and session authorization.

Syntax

`set tacacs session accounting` {**`enable`** | **`disable`**}

set tacacs session authorization {**`service`** *name* | **`read-only`** *attribute value* | **`read-write`** *attribute value* | **`super-user`** *attribute value*}

Parameters

accounting	Specifies that TACACS+ session accounting is being configured.
enable | **disable**	Enables or disables TACACS+ session accounting.
authorization	Specifies that TACACS+ session authorization is being configured.
service *name*	Specifies the name of the service that the TACACS+ client will request from the TACACS+ server. The *name* specified here must match the name of a service configured on the server.
read-only *attribute value*	Specifies that the Matrix **read-only** access privilege level should be matched to a privilege level configured on the TACACS+ server by means of an attribute-value pair specified by *attribute* and *value*. By default, *attribute* is "priv-lvl" and *value* is 0.
read-write *attribute value*	Specifies that the Matrix **read-write** access privilege level should be matched to a privilege level configured on the TACACS+ server by means of an attribute-value pair specified by *attribute* and *value*. By default, *attribute* is "priv-lvl" and *value* is 1.
super-user *attribute value*	Specifies that the Matrix **super-user** access privilege level should be matched to a privilege level configured on the TACACS+ server by means of an attribute-value pair specified by *attribute* and *value*. By default, *attribute* is "priv-lvl" and *value* is 15.

Defaults

None.

Downloaded from www.Manualslib.com manuals search engine

Mode

Switch command, Read-Write.

Usage

When session accounting is enabled, the TACACS+ server will log accounting information, such as start and stop times, IP address of the client, and so forth, for each authorized client session.

When the TACACS+ client is enabled on the Enterasys Matrix switch (with the **set tacacs enable** command), the session authorization parameters configured with this command are sent by the client to the TACACS+ server when a session is initiated on the Enterasys Matrix switch. The parameter values must match a service and access level attribute-value pairs configured on the server for the session to be authorized. If the parameter values do not match, the session will not be allowed.

The service name and attribute-value pairs can be any character string, and are determined by your TACACS+ server configuration.

Examples

This example configures the service requested by the TACACS+ client as the service name “basic.”

```
Matrix(rw)->set tacacs session authorization service basic
```

This example maps the Matrix **read-write** access privilege level to an attribute named “priv-lvl” with the value of 5 configured on the TACACS+ server.

```
Matrix(rw)->set tacacs session authorization read-write priv-lvl 5
```

This example enables TACACS+ session accounting.

```
Matrix(rw)->set tacacs session accounting enable
```

clear tacacs session

Use this command to return the TACACS+ session authorization settings to their default values.

Syntax

clear tacacs session authorization { [**service**] [**read-only**] [**read-write**] [**super-user**] }

Parameters

authorization	Clears the TACACS+ session authorization parameters.
service	Clears the TACACS+ session authorization service name to the default value of “exec.”
read-only	Clears the TACACS+ session authorization read-only attribute-value pair to their default values of “priv-lvl” and 0.
read-write	Clears the TACACS+ session authorization read-write attribute-value pair to their default values of “priv-lvl” and 1.
super-user	Clears the TACACS+ session authorization super-user attribute-value pair to their default values of “priv-lvl” and 15.

Downloaded from www.Manualslib.com manuals search engine

Defaults

At least one of the session authorization parameters must be specified.

Mode

Switch command, Read-Write.

Examples

This example shows how to return only the service name to the default of “exec.”

```
Matrix(rw)->clear tacacs session authorization service
```

This example shows how to return all the session authorization parameters to their default values.

```
Matrix(rw)->clear tacacs session authorization service read-only read-write
super-user
```

show tacacs command

Use this command to display the status (enabled or disabled) of TACACS+ accounting or authorization on a per-command basis.

Syntax

show tacacs command {**accounting** | **authorization**} [**state**]

Parameters

accounting	Display the status of TACACS+ accounting on a per-command basis.
authorization	Display the status of TACACS+ authorization on a per-command basis.
state	(Optional) Specifies that only the status should be displayed.

Defaults

If **state** is not specified, all accounting or authorization configuration parameters are displayed (which at this time includes only the enabled/disabled status).

Mode

Switch command, Read-Write.

Example

This example shows how to display the state of the TACACS+ client’s command authorization.

```
Matrix(rw)->show tacacs command authorization
TACACS+ command authorization state:  enabled
```


Downloaded from www.Manualslib.com manuals search engine

set tacacs command

Use this command to enable or disable TACACS+ accounting or authorization on a per-command basis.

Syntax

```
set tacacs command {accounting | authorization} {enable | disable}
```

Parameters

accounting | authorization	Specifies either TACACS+ accounting or authorization to be enabled or disabled.
enable | disable	Enable or disable accounting or authorization on a per-command basis.

Defaults

None.

Mode

Switch command, Read-Write.

Usage

In order for per-command accounting or authorization by a TACACS+ server to take place, the command must be executed within an authorized session.

When per-command accounting is enabled, the TACACS+ server will log accounting information, such as start and stop times, IP address of the client, and so forth, for each command executed during the session.

When per-command authorization is enabled, the TACACS+ server will check whether each command is permitted for that authorized session and return a success or fail. If the authorization fails, the command is not executed.

Example

This example shows how to enable TACACS+ authorization on a command basis.

```
Matrix(rw)->set tacacs command authorization enable
```

show tacacs singleconnect

Use this command to display the current status of the TACACS+ client's ability to send multiple requests over a single TCP connection.

Syntax

```
show tacacs singleconnect [state]
```

Parameters

state	(Optional) Specifies that only the single connection state should be displayed.

Downloaded from www.Manualslib.com manuals search engine

Defaults

If **state** is not specified, all single connection configuration parameters are displayed (which at this time includes only the enabled/disabled state).

Mode

Switch command, Read-Write.

Example

This example shows how to display the state of the TACACS+ client's ability to send multiple requests over a single connection.

```
Matrix(rw)->show tacacs singleconnect
  TACACS+ single-connect state:         enabled
```

set tacacs singleconnect

Use this command to enable or disable the ability of the TACACS+ client to send multiple requests over a single TCP connection. When enabled, the TACACS+ client will use a single TCP connection for all requests to a given TACACS+ server.

Syntax

set tacacs singleconnect {**enable** | **disable**}

Parameters

enable | disable	Enable or disable the ability to send multiple requests over a single TCP connection.

Defaults

None.

Mode

Switch command, Read-Write.

Examples

This example shows how to disable sending multiple requests over a single connection.

```
Matrix(rw)->set tacacs singleconnect disable
```


Downloaded from www.Manualslib.com manuals search engine

26

RADIUS Snooping Configuration

This chapter describes the RADIUS Snooping commands and how to use them.



Note: An Enterasys Feature Guide document that contains a complete discussion on RADIUS Snooping configuration exists at the following Enterasys web site: http://www.enterasys.com/support/manuals/

Understanding RADIUS Snooper

RADIUS Snooper (RS) allows a network manager to manage downstream connections, when the full complement of Enterasys' SecureNetworks capabilities is not deployed at the network edge. This allows for the deployment of less feature rich edge devices to perform basic access control at the network edge, while still providing complex user and service based CoS provisioning, authorization, and usage auditing to the session.

Many downstream devices authenticate the local session with a RADIUS server that resides upstream of the distribution-tier device. RADIUS request and response frames from these devices transit the distribution-tier device. The interception of this RADIUS traffic allows the distribution-tier device to build an authenticated session for the end-station, as though it was directly connected. Sessions detected by RS function identically to local authenticated sessions from the perspective of the Enterasys MultiAuth framework.

The unencrypted traffic of the downstream devices passes through the device running RS, allowing such MultiAuth and SecureNetwork features as session-timeout, idle-timeout, filter-ID attributes and VLAN-tunnel attributes to be applied to the traffic.

The client sends a RADIUS Access-Request frame to the RADIUS server to initiate the authentication process. This request frame contains the Calling-Station-ID attribute. The Calling-Station-ID, containing the MAC address, is captured by the RS. The session is defined by the attributes returned by the RADIUS server in the Access-Accept frame. The idle-timeout and session-timeout dictate the end of the session, just as if the session was directly connected to the distributed-tier device running RS.

The RS flow table contains flows for each valid session for this system. The client IP address and authenticating RADIUS server IP address are manually entered into the RADIUS flow table on the RS enabled switch. When an investigated RADIUS frame transits the RS enabled port with a match in the flow table, a session is created. The session becomes active when it sees a response for the session match from the RADIUS server.

A configurable timer determines the amount of time the firmware will wait before terminating a session because no response was seen from the RADIUS server.

Default and network administrator configurable RADIUS packet drop settings exist based upon resource issues and validation failure. Packet drop for validation failures can be configured on a port-by-port basis.

To configure RS on a switch:

Downloaded from www.Manualslib.com manuals search engine

- Globally enable RS on the switch
- Enable RS on those ports you wish enabled for snooping
- Optionally change the period RS will wait for a RADIUS response frame from the server
- Manually populate the RADIUS flow table with RS clients and RADIUS servers

Command options also are available to:

- Terminate all sessions on the system for the specified port or for the specified MAC address
- Reset all RS configuration to the default values
- Clear all RS counters
- Clear flows from all or the specified flow table
- Display RS statistics

Purpose

To enable, configure and display information for RADIUS Snooping used by the network manager to manage downstream connections, when the full complement of Enterasys' SecureNetworks capabilities is not deployed at the network edge.

Commands

For information about...	Refer to page...
set radius-snooping	26-2
set radius-snooping timeout	26-3
set radius-snooping port	26-4
set radius-snooping flow	26-5
set radius-snooping initialize	26-6
clear radius-snooping all	26-6
clear radius-snooping flow	26-7
clear radius-snooping flow	26-7
show radius-snooping	26-7
show radius-snooping port	26-8
show radius-snooping flow	26-9
show radius-snooping session	26-10

set radius-snooping

Use this command to globally enable or disable RS for this device.

Syntax

```
set radius-snooping {enable | disable}
```


Downloaded from www.Manualslib.com manuals search engine

Parameters

enable	Globally enables RS on this device.
disable	Globally disables RS on this device.

Defaults

None.

Mode

Read-Write.

Usage

This command does not enable RS on the ports for this device. To enable ports for RS see the command *set radius-snooping port* on page 26-4.

Example

This example shows how to enable RS on this device:

```
Matrix(rw)->set radius-snooping enable
```

set radius-snooping timeout

Use this command to set the number of seconds that the firmware waits for a RADIUS response frame to be returned from the RADIUS server, after successfully snooping a RADIUS request frame from the client.

Syntax

set radius-snooping timeout *seconds*

Parameters

seconds	Specifies the number of seconds that the firmware waits from the time it successfully snoops a RADIUS request frame, for a RADIUS response frame to be returned from the RADIUS server. Default: **20**

Defaults

None.

Mode

Read-Write.

Usage

If no response is seen before the timeout expires, the session is terminated.

Radius-Snooper timeout values are rounded to the nearest factor of 10. For example, a configured value of 22 would be an actual value of 20.

Downloaded from www.Manualslib.com manuals search engine

Example

This example shows how to set the RS timeout to 30 seconds:

```
Matrix(rw)->set radius-snooping timeout 30
```

set radius-snooping port

Use this command to enable RS on all or the specified port(s).

Syntax

set radius-snooping port [**enable** | **disable**] [**timeout** *seconds*] [**drop** {**enable** | **disable**}] [**authallocated** *number*] [*port-string*]

Parameters

enable | **disable**	Enables or disables RS functionality on the specified port(s). Disabled by default.
timeout *seconds*	Specifies the number of seconds the firmware waits for a RADIUS response frame after it successfully snoops a RADIUS request frame. The timeout timer defaults to 0 seconds (unset). When 0 seconds is configured, the firmware uses the system level timeout value.
drop {enable | disable}	Sets the RADIUS traffic drop behavior for this port. Disabled by default.
authallocated *number*	Sets the number of allowed RS sessions allowed on a per port basis. Default value is 8, 128, or 256 depending upon the system license for this device.
port-string	Enables RS for the specified port(s).

Defaults

If no timeout value is specified, the global timeout value specified in the **set radius-snooping timeout** command is used.

If no parameters are specified, RADIUS snooping is enabled on all ports.

Mode

Read-write.

Usage

If the timeout timer expires, the affected session is terminated. If timeout is set to **0**, the global timeout is used.

Set the authallocated value equal to or less than the configured value for **set multiauth port numusers**. This value is the maximum number of users per port for all authentication clients.

In some cases it may be necessary to drop RADIUS traffic in order to maintain session consistency between the distribution tier device and the edge switches. Packets are always dropped for a resource issue situation. With drop enabled, frames with an invalid calling station ID are also dropped.

Downloaded from www.Manualslib.com manuals search engine

Example

This example enables RS on ports ge.1.10 through ge.1.15, sets the timeout to 15 seconds and enables drop:

```
Matrix(rw)->set radius-snooping enable timeout 15 drop enable ge.1.10-15
```

set radius-snooping flow

Use this command to provide for the entering of RADIUS client and server session flow entries into the RS flow table.

Syntax

set radius-snooping flow *index client-IP-Address server-IP-Address* {**port** | **standard**} [*secret*]

Parameters

index	Specifies a numeric index ID for this flow table entry.
client-IP-Address	Specifies the client IP address for this RS flow table entry.
server-IP-Address	Specifies the server IP address for this RS flow table entry.
port	Specifies the RADIUS UDP port to use for this RS flow table entry.
standard	Specifies RADIUS UDP standard port 1812.
secret	Specifies the RADIUS secret for this RS flow table entry.

Defaults

If no **secret** is specified, no secret is used for this flow entry.

Mode

Read-write.

Usage

RADIUS flows defined in the RS flow table are snooped if RS is enabled for both the system and this port.

Flow entries are added to the flow table based upon the entry index value. The first matching entry in the table is the entry used for the continuation of the authentication process.

If a secret is configured on the authentication server and not configured here, no validation will occur.

Example

This example creates an index 1 entry in the RADIUS flow table for client **192.10.5.10** and server **192.10.20.1** for the standard UPD port 1812 with a secret **mysecret**:

```
Matrix(rw)->set radius-snooping flow 1 192.10.5.10 192.10.20.1 standard mysecret
```


Downloaded from www.Manualslib.com manuals search engine

set radius-snooping initialize

Use this command to terminate all RS sessions on the system for the specified port or MAC address.

Syntax

set radius-snooping initialize {**port** *port-string* | *mac-address*}

Parameters

port *port-string*	Specifies the port(s) to initialize. Use *.*.* for all ports.
mac-address	Specifies the MAC address to initialize.

Defaults

None.

Mode

Read-write.

Example

This example terminates all RS sessions associated with port **ge.1.1** by initializing the port:

```
Matrix(rw)->set radius-snooping initialize port ge.1.1
```

clear radius-snooping all

Use this command to reset all RS configuration to the default values for this system.

Syntax

clear radius-snooping all

Parameters

None.

Defaults

None.

Mode

Read-Write.

Example

This example resets all RS configuration to the default setting for this system:

```
Matrix(rw)->clear radius-snooping all
```


Downloaded from www.Manualslib.com manuals search engine

clear radius-snooping flow

Use this command to clear all entries or the specified index entry from the RS flow table.

Syntax

clear radius-snooping flow {**all** | *index*}

Parameters

all	Specifies that all flow table entries are to be cleared.
index	Specifies a specific flow table index entry to be cleared.

Defaults

None.

Mode

Read-write.

Usage

Use the *index* value to clear flows for a particular port.

Examples

This example clears all flow table entries:

```
Matrix(rw)->clear radius-snooping flow all
```

This example clears the flow table entry for index 5:

```
Matrix(rw)->clear radius-snooping flow 5
```

show radius-snooping

Use this command to display a general overview of the global RS status.

Syntax

show radius-snooping

Parameters

None.

Defaults

None.

Mode

Read-Only.

Downloaded from www.Manualslib.com manuals search engine

Example

This example shows how to display RADIUS configuration information:

```
Matrix(rw)->show radius-snooping
RADIUS Snooping: Enabled
Number of configured flows:    2
Active sessions: 12

Enabled ports: fe.1.1-fe.1.8; fe.1.22
```

Table 26-1 Radius-Snooping Settings

Output...	What it displays...
RADIUS Snooping	Specifies whether RS is globally enabled or disabled.
Number of configured flows	Specifies the number of globally configured flows for this system.
Active sessions	Specifies the number of active sessions for this system.
Enabled ports	Specifies the ports RS is currently enabled on.

show radius-snooping port

Use this command to display both a general overview of the global RS status as well as the per port RS status for the port(s) specified.

Syntax

show radius-snooping port *port-string*

Parameters

port-string	Specifies the port for status to be displayed.

Defaults

None.

Mode

Read-Only.

Example

This example displays the RS status for port **fe.1.1**:

```
Matrix(rw)->show radius-snooping port fe.1.1
Radius-Snooping: Enabled

Port   Port State Timeout Drop State Allowed Allocated
fe.1.1 disabled   40      enabled    1024    1024
```


Downloaded from www.Manualslib.com manuals search engine

Table 26-2 Radius-Snooping Port Settings

Output...	What it displays...
Port	Specifies the port(s) currently enabled for RS.
Port State	Specifies the actual port state.
Timeout	Specifies the amount of time in seconds before the session will be terminated if no response is seen from the RADIUS server once a request is seen from the client.
Drop State	Specifies whether Drop State is enabled or disabled for sessions on this port.
Allowed	Specifies the maximum number of sessions allowed by license for this port.
Allocated	Specifies the number of allocated sessions as set in the command *set radius-snooping port* on page 26-4.

show radius-snooping flow

Use this command to display information for all flows or the specified index entry in the flow table.

Syntax

show radius-snooping flow {*index* | **all**}

Parameters

index	Specifies a specific flow table index entry to be displayed.
all	Specifies that all flow table entries are to be displayed.

Defaults

None.

Mode

Read-Write.

Usage

Use the *index* to specify a particular flow to display, otherwise use **all**.

Example

This example displays the flow information for index **1**:

```
Matrix(rw)->show radius-snooping flow 1
FlowID  Client IP      Server IP      UDP Port  Validation
1       192.10.20.5    192.10.10.10   1812      Enabled

Number of current sessions     : 17
Number pending                 : 4

Total Sessions:                : 85
Total RADIUS Access Requests   : 242
```


Downloaded from www.Manualslib.com manuals search engine

```
Total RADIUS Access Accepts    : 212
Total RADIUS Access Rejects    : 26
Invalid RADIUS Request packets : 0
Invalid RADIUS Response packets: 0
Total Dropped Packets          : 0
```

Table 26-3 Radius-Snooping Flow Settings

Output...	What it displays...
FlowID	Specifies the index ID for this flow.
Client IP	Specifies the client IP address for this flow.
Server IP	Specifies the server IP address for this flow.
UDP Port	Specifies the authentication server UDP port for this flow.
Validation	Specifies enabled if there is a secret configured, otherwise specifies disabled. For security reasons the secret does not display.
Number of current sessions	Specifies the number of active sessions for this flow.
Number pending	Specifies the number of valid RADIUS request frames pending, but no matching RADIUS response frame has been seen. These sessions are currently inactive.
Total Sessions	Specifies the total number of sessions on this system.
Total RADIUS Access Requests	Specifies the total number of RADIUS access requests seen by RS on this system.
Total RADIUS Access Rejects	Specifies the total number of RADIUS response reject frames seen by RS on this system.
Invalid RADIUS Request Packets	Specifies the total number of RADIUS request frames seen by the RS on this system.
Invalid RADIUS Response Packets	Specifies the total number of Invalid RADIUS response frames seen by RS on this system. An invalid frame is generated when request frames do not contain the necessary attributes with the required values for successful processing.
Total Dropped Packets	Specifies the total number of frames dropped by RS on this system.

show radius-snooping session

Use this command to display an RS summary for all sessions or the specified port or MAC address criteria.

Syntax

show radius-snooping session {**port** *port-string* | **mac** *mac-address*}

Parameters

port *port-string*	Specifies the port(s) session to display. Enter *.*.* for all ports.
mac *mac-address*	Specifies the MAC address session to display

Downloaded from www.Manualslib.com manuals search engine

Defaults

None.

Mode

Read-Only.

Examples

This example displays RADIUS configuration information for port **fe.1.1**:

```
Matrix(rw)->show radius-snooping session port fe.1.1
Port    MAC Address        Duration
fe.1.1  00-0E-0C-12-13-14  00:02:36
```

Table 26-4 Radius-Snooping Session Port Settings

Output...	What it displays...
MAC Address	Specifies the MAC address associated with the session information in this display.
Port	Specifies the port ID associated with the session information in this display.
Duration	Specifies the length of time this session has been active.

```
Matrix(rw)->show radius-snooping session 00-00-44-44-00-04
          MAC Address:    00-00-44-44-00-04
          Port:                      fe.2.8
          Duration:             0, 00:01:47

          Downstream Device IP:  10.21.64.70
          RADIUS Server IP:      10.21.1.150
```

Table 26-5 Radius-Snooping Session MAC Settings

Output...	What it displays...
Port	Specifies the port associated with this MAC address.
MAC Address	Specifies the MAC Address for this session.
Duration	Specifies the length of time that this session has been active.
Downstream device IP	Specifies the IP address of the client associated with this session.
Radius Server IP	Specifies the IP address of the RADIUS server for this session.

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

27

MultiAuth Configuration

This chapter describes the MultiAuth set of commands and how to use them. Multiple User Multiple Authentication – allows multiple users on a given port to simultaneously authenticate using any or all of the supported protocols (MAC Authentication, PWA, 802.1X, and CEP), and for each authenticated user to receive a unique level of network access.

Note: An Enterasys Feature Guide document that contains a complete discussion on authentication configuration, including MultiAuth, exists at the following Enterasys web site: http://www.enterasys.com/support/manuals/

Configuring Multiple Authentication

About Multiple Authentication

When enabled, multiple authentication allows multiple users to authenticate using up to three methods on the same port, and receive a policy traffic profile based on the RADIUS configuration. When multi-authentication ports have a combination of authentication methods enabled, and a user is successfully authenticated in more than one way at the same time, the precedence of the authentication methods will determine which RADIUS-returned filter ID will be processed and result in an applied traffic policy profile.

DFE-Gold Multi-User Capacities

Matrix DFE Gold modules support one authenticated user and one IP phone per port. The system (chassis) supports up to 1024 authenticated users.

The number of authenticated users allowed per port can be controlled by means of the *set multiauth port* on page 27-6.

Purpose

To configure multiple authentication.

Note: In order for multiple authentication to function on the device, each possible method of authentication (MAC authentication, PWA, 802.1X) must be enabled globally and configured appropriately on the desired ports per its corresponding command set as described in this chapter.

Multiple authentication mode must be globally enabled on the device using the **set multiauth mode** command as described in “set multiauth mode” on page 27-2.

Downloaded from www.Manualslib.com manuals search engine

Commands

For information about...	Refer to page...
set multiauth mode	27-2
clear multiauth mode	27-3
show multiauth	27-3
show multiauth counters	27-4
set multiauth precedence	27-5
clear multiauth precedence	27-5
show multiauth port	27-6
set multiauth port	27-6
clear multiauth port	27-7
show multiauth station	27-8
clear multiauth station	27-8
show multiauth session	27-9
show multiauth idle-timeout	27-10
set multiauth idle-timeout	27-10
clear multiauth idle-timeout	27-11
show multiauth session-timeout	27-12
set multiauth session-timeout	27-13
clear multiauth session-timeout	27-14
set multiauth trap	27-14
clear multiauth trap	27-15
show multiauth trap	27-16

set multiauth mode

Use this command to set the system authentication mode to use multiple authenticators simultaneously or to strictly adhere to 802.1X.

Syntax

```
set multiauth mode {multi | strict}
```

Parameters

multi	Allows the system to use multiple authenticators simultaneously. **Note:** This mode requires that MAC, PWA, and 802.1X authentication be enabled globally, and configured appropriately on the desired ports per its corresponding command set as described in this chapter.
strict	Sets the system authentication mode to strict 802.1X.

Downloaded from www.Manualslib.com manuals search engine

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to enable multiple authentication:

```
Matrix(rw)->set multiauth mode multi
```

clear multiauth mode

Use this command to clear the system authentication mode.

Syntax

clear multiauth mode

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to clear the system authentication mode:

```
Matrix(rw)->clear multiauth mode
```

show multiauth

Use this command to display system-configured multiauth values.

Syntax

show multiauth

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Only.

Downloaded from www.Manualslib.com manuals search engine

Example

This example shows how to display multiple authentication session-timeout values, for an active session:

```
Matrix(su)->show multiauth
Multiple authentication system configuration
-------------------------------------------------
Supported types               : dot1x, pwa, mac, cep
Maximum number of users       : 2048
Current number of users       : 1
System mode                   : multi
Default precedence            : dot1x, pwa, mac, cep
Admin precedence              : dot1x, mac, pwa, cep
Operational precedence        : dot1x, mac, pwa, cep
```

show multiauth counters

Use this command to display multiauth counter values.

Syntax

show multiauth counters [[**cep** | **dot1x** | **mac** | **pwa**][**chassis** | **port** *portstring*]] [[**chassis** [**cep** | **dot1x** | **mac** | **pwa**]] [**port** *portstring*]

Parameters

portstring	Specifies a port or range of ports to display.

Defaults

Displays multiauth counter information for all parameters.

Mode

Switch command, Read-Only.

Example

This example shows how to display multiple authentication session-timeout values, for an active session:

```
Matrix(su)->show multiauth counters
Location   Authentication Type
           dot1x      pwa        mac        cep
           ---------- ---------- ---------- ----------
chassis    0          0          0          0
ge.1.1     0          0          0          0
ge.1.2     0          0          0          0
.
.
.
lag.0.45   0          0          0          0
```


Downloaded from www.Manualslib.com manuals search engine

```
lag.0.46    0           0           0           0
lag.0.47    0           0           0           0
lag.0.48    0           0           0           0
```

set multiauth precedence

Use this command to set the system's multiple authentication administrative precedence.

Syntax

set multiauth precedence {[**dot1x**] [**mac**] [**pwa**] [**cep**]}

Parameters

dot1x	Sets precedence for 802.1X authentication.
mac	Sets precedence for MAC authentication.
pwa	Sets precedence for port web authentication.
cep	Sets precedence for CEP authentication

Defaults

From high to low precedence: **dot1x**, **pwa**, **mac**, **cep**.

Mode

Switch command, Read-Write.

Usage

When a user is successfully authenticated by more than one method at the same time, the precedence of the authentication methods will determine which RADIUS-returned filter ID will be processed and result in an applied traffic policy profile.

Example

This example shows how to set precedence for MAC authentication:

```
Matrix(rw)->set multiauth precedence mac
```

clear multiauth precedence

Use this command to clear the system's multiple authentication administrative precedence.

Syntax

clear multiauth precedence

Parameters

None.

Defaults

None.

Downloaded from www.Manualslib.com manuals search engine

Mode

Switch command, Read-Write.

Example

This example shows how to clear the multiple authentication precedence:

```
Matrix(rw)->clear multiauth precedence
```

show multiauth port

Use this command to display multiple authentication properties for one or more ports.

Syntax

show multiauth port [*port-string*]

Parameters

port-string	(Optional) Displays multiple authentication information for specific port(s).

Defaults

If *port-string* is not specified, multiple authentication information will be displayed for all ports.

Mode

Switch command, Read-Only.

Example

This example shows how to display multiple authentication information for ports fe.1.1-4:

```
Matrix(rw)->show multiauth port fe.1.1-4
Port         Mode           Max       Allowed    Current
                           users       users      users
------------ ------------- ---------- ---------- ----------
fe.1.1       auth-opt      128        128        0
fe.1.2       auth-opt      128        128        0
fe.1.3       auth-opt      128        128        0
fe.1.4       auth-opt      128        128        0
```

set multiauth port

Use this command to set multiple authentication properties for one or more ports.

Syntax

set multiauth port mode {**auth-opt** | **auth-reqd** | **force-auth** | **force-unauth**} | **numusers** *numusers port-string*

Downloaded from www.Manualslib.com manuals search engine

Parameters

mode auth-opt | **auth-reqd** | **force-auth** | **force-unauth**	Specifies the port(s)' multiple authentication mode as: • **auth-opt** — Authentication optional • **auth-reqd** — Authentication required • **force-auth** — Authentication considered • **force-unauth** — Authentication disabled
numusers *numusers*	Specifies the number of users allowed authentication on port(s).
port-string	Specifies the port(s) on which to set multiple authentication properties.

Defaults

None.

Mode

Switch command, Read-Write.

Examples

This example shows how to set the port multiple authentication mode to required on ge.3.14:

```
Matrix(rw)->set multiauth port mode auth-reqd ge.3.14
```

clear multiauth port

Use this command to clear multiple authentication properties for one or more ports.

Syntax

clear multiauth port {[**mode**] [**numusers**] *port-string*}

Parameters

mode	Clears the port(s)' multiple authentication mode.
numusers	Clears the value set for the number of users allowed authentication on port(s).
port-string	Specifies the port(s) on which to clear multiple authentication properties.

Defaults

None.

Mode

Switch command, Read-Write.

Examples

This example shows how to clear the port multiple authentication mode on all 1-Gigabit Ethernet ports:

```
Matrix(rw)->clear multiauth port mode ge.*.*
```


Downloaded from www.Manualslib.com manuals search engine

show multiauth station

Use this command to display multiple authentication station (end user) entries.

Syntax

show multiauth station [**mac** *address*] [**port** *port-string*]

Parameters

mac *address*	(Optional) Displays multiple authentication station entries for specific MAC address(es).
port *port-string*	(Optional) Displays multiple authentication station entries for specific port(s).

Defaults

If no options are specified, multiple authentication station entries will be displayed for all MAC addresses and ports.

Mode

Switch command, Read-Only.

Example

This example shows how to display multiple authentication station entries. In this case, two end user MAC addresses are shown:

```
Matrix(rw)->show multiauth station
Port         Address type Address
------------ ------------ ------------------------
fe.1.20 mac          00-10-a4-9e-24-87
fe.2.16 mac          00-b0-d0-e5-0c-d0
```

clear multiauth station

Use this command to clear one or more multiple authentication station entries.

Syntax

clear multiauth station [**mac** *address*] **port** *port-string*

Parameters

mac *address*	(Optional) Clears multiple authentication station entries for specific MAC address(es).
port *port-string*	Specifies the port(s) for which to clear multiple authentication station entries.

Defaults

If not specified, multiple authentication station entries will be cleared for all MAC addresses.

Downloaded from www.Manualslib.com manuals search engine

Mode

Switch command, Read-Write.

Example

This example shows how to clear the multiple authentication station entry associated with port fe.1.20:

```
Matrix(rw)->clear multiauth station port fe.1.20
```

show multiauth session

Use this command to display multiple authentication session entries.

Syntax

show multiauth session [**all**] [**agent** {**dot1x** | **mac** | **pwa** | **cep**}] [**mac** *address*] [**port** *port-string*]

Parameters

all	(Optional) Displays information about all sessions, including those with terminated status.
agent | **dot1x** | **mac** | **pwa** | **cep**	(Optional) Displays 802.1X, MAC, CEP, or port web authentication session information.
mac *address*	(Optional) Displays multiple authentication session entries for specific MAC address(es).
port *port-string*	(Optional) Displays multiple authentication session entries for specific port(s).

Defaults

If no options are specified, multiple authentication session entries will be displayed for all sessions, authentication types, MAC addresses, and ports.

Mode

Switch command, Read-Only.

Example

This example shows how to display multiple authentication session:

```
Matrix(rw)->show multiauth session
Multiple authentication session entries
----------------------------------------
Port            : fe.2.2         Station address   : 00-01-f4-2b-4f-8b
Auth status     : success        Last attempt      : MON MAY 08 14:34:42 2006
Agent type      : pwa            Session applied   : true
Server type     : radius         VLAN-Tunnel-Attr  : None
Policy index    : 0              Policy name       : No policy applied
Session timeout : 43200          Session duration  : 0,00:01:01
Idle timeout    : 300            Idle time         : 0,00:00:00
```


Downloaded from www.Manualslib.com manuals search engine

```
Termination time: Not Terminated
```

show multiauth idle-timeout

Use this command to display the multiple authentication timeout value for an idle session.

Syntax

show multiauth idle-timeout

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Only.

Usage

This will display the idle-timeout values, in seconds, for the following authentication types: dot1x, pwa, mac, and cep.

Example

This example shows how to display timeout values for an idle session, for each of the authentication types:

```
Matrix(rw)->show multiauth idle-timeout
Authentication type  Timeout (sec)
-------------------- -------------
dot1x                300
pwa                  300
mac                  300
cep                  300
```

set multiauth idle-timeout

Use this command to set the multiauth idle-timeout value per authentication method or for all methods.

Syntax

set multiauth idle-timeout [**cep** | **dot1x** | **mac** | **pwa**] *timeout*

Parameters

cep	(Optional) Specifies the authentication type Enterasys Convergence End Point Authentication.
dot1x	(Optional) Specifies the authentication type IEEE 802.1X Port-Based Network Access Control.

Downloaded from www.Manualslib.com manuals search engine

mac	(Optional) Specifies the authentication type Enterasys Mac Authentication.
pwa	(Optional) Specifies the authentication type Enterasys Port Web Authentication.
timeout	Specifies the timeout value in seconds. The value can range from 0 to 65535. A value of 0 means that no idle timeout will be applied unless an idle timeout value is provided by the authenticating server. The default timeout value is 300 seconds.

Defaults

If no authentication method is specified, the timeout value is set for all methods.

Mode

Switch command, Read-Write.

Usage

A value of zero indicates that no idle timeout will be applied unless an idle timeout value is provided by the authenticating server. For example, if a session is authenticated by a RADIUS server, that server may encode a Idle-Timeout Attribute in its authentication response.

Examples

This example shows how to set the idle-timeout session for cep and mac authentication to 500 seconds:

```
Matrix(rw)->set multiauth idle-timeout cep 500
Matrix(rw)->set multiauth idle-timeout mac 500
```

This example shows how to set the idle-timeout session for all the authentication types to 600 seconds:

```
Matrix(rw)->set multiauth idle-timeout 600
```

clear multiauth idle-timeout

Use this command to reset the maximum number of consecutive seconds an authenticated session may be idle before termination of the session to the default value of 300 seconds.

Syntax

clear multiauth idle-timeout [**cep** | **dot1x** | **mac** | **pwa**]

Parameters

cep	(Optional) Specifies the authentication type Enterasys Convergence End Point Authentication.
dot1x	(Optional) Specifies the authentication type IEEE 802.1X Port-Based Network Access Control.
mac	(Optional) Specifies the authentication type Enterasys Mac Authentication.
pwa	(Optional) Specifies the authentication type Enterasys Port Web Authentication.

Downloaded from www.Manualslib.com manuals search engine

Defaults

If no authentication type is specified, the idle timeout value is returned to 300 seconds for all authentication types.

Mode

Switch command, Read-Write.

Examples

This example shows how to clear the idle-timeout session values for cep and mac authentication types, back to default value of 300 seconds:

```
Matrix(rw)->clear multiauth idle-timeout cep
Matrix(rw)->clear multiauth idle-timeout mac
```

This example shows how to clear the idle-timeout session values for all authentication types, back to the default value of 300 seconds:

```
Matrix(rw)->set multiauth idle-timeout
```

show multiauth session-timeout

Use this command to display session-timeout values, in seconds, for all authentication methods.

Syntax

`show multiauth session-timeout`

Parameters

None

Defaults

None.

Mode

Switch command, Read-Only.

Example

This example shows how to display multiple authentication session-timeout values, for an active session:

```
Matrix(rw)->show multiauth session-timeout
Authentication type  Timeout (sec)
-------------------- -------------
dot1x                0
pwa                  0
mac                  0
cep                  0
```


Downloaded from www.Manualslib.com manuals search engine

set multiauth session-timeout

Use this command to set the maximum number of seconds an authenticated session may last before termination of the session.

Syntax

set multiauth session-timeout [**cep** | **dot1x** | **mac** | **pwa**] *timeout*

Parameters

cep	(Optional) Specifies the authentication type Enterasys Convergence End Point Authentication.
dot1x	(Optional) Specifies the authentication type IEEE 802.1X Port-Based Network Access Control.
mac	(Optional) Specifies the authentication type Enterasys Mac Authentication.
pwa	(Optional) Specifies the authentication type Enterasys Port Web Authentication.
timeout	Specifies the timeout value in seconds. The value can range from 0 to 65535. A value of 0 means that no session timeout will be applied unless a session timeout value is provided by the authenticating server.

Defaults

If no authentication type is specified, the timeout value is set for all types.

Mode

Switch command, Read-Write.

Usage

A value of zero may be superseded by a session timeout value provided by the authenticating server. For example, if a session is authenticated by a RADIUS server, that server may encode a Session-Timeout Attribute in its authentication response.

Examples

This example shows how to set the session-timeout value for an active session, for cep and mac authentication to 500 seconds:

```
Matrix(rw)->set multiauth session-timeout cep 500
Matrix(rw)->set multiauth session-timeout mac 500
```

This example shows how to set the session-timeout value for an active session, for all the authentication types to 600 seconds:

```
Matrix(rw)->set multiauth session-timeout 600
```


Downloaded from www.Manualslib.com manuals search engine

clear multiauth session-timeout

Use this command to clear session-timeout values, for one or all authentication methods, back to the default values.

Syntax

clear multiauth session-timeout [**cep** | **dot1x** | **mac** | **pwa**]

Parameters

cep	(Optional) Specifies the authentication type Enterasys Convergence End Point Authentication.
dot1x	(Optional) Specifies the authentication type IEEE 802.1X Port-Based Network Access Control.
mac	(Optional) Specifies the authentication type Enterasys Mac Authentication.
pwa	(Optional) Specifies the authentication type Enterasys Port Web Authentication.

Defaults

If no authentication type is specified, the session timeout value is returned to 300 seconds for all authentication types.

Mode

Switch command, Read-Write.

Examples

This example shows how to clear the session-timeout values, for an active session, for cep and mac authentication types, to the default value of 0 seconds:

```
Matrix(rw)->clear multiauth idle-timeout cep
Matrix(rw)->clear multiauth idle-timeout mac
```

This example shows how to clear the session-timeout values, for an active session, for all authentication types, to the default value of 0 seconds:

```
Matrix(rw)->set multiauth idle-timeout
```

set multiauth trap

Use this command to set the multiauth trap setting for system, module and port.

Syntax

set multiauth trap {**system** {**enabled** | **disabled**} | **module** {**enabled** | **disabled**} | **port** *portstring* {**all** | **success** | **failed** | **terminated** | **max-reached**}}

Downloaded from www.Manualslib.com manuals search engine

Parameters

system	Configures multiauth system trap settings as follows: **enabled** - traps are sent when max users reached in system **disabled** - traps are not sent when max users reached in system
module	Configures multiauth module trap settings as follows: **enabled** - traps are sent when max users reached in module **disabled** - traps are not sent when max users reached in module
port *portstring*	Configures multiauth port trap settings for the port specified in *portstring*.
all	Enables sending all traps for the specified port.
success	Enables sending success traps for the specified port.
failed	Enables sending failed traps for the specified port.
terminated	Enables sending terminated traps for the specified port.
max-reached	Enables sending max number users reached traps for the specified port.

Defaults

All sending of multiauth traps disabled.

Mode

Switch command, Read-Write.

Examples

This example shows how to enable the multiauth system trap setting:

```
Matrix(rw)->set multiauth trap system enabled
```

This example shows how to enable all multiauth port trap setting:

```
Matrix(rw)->set multiauth trap port ge.1.1 all
```

clear multiauth trap

Use this command to clear the system's multiple authentication trap settings.

Syntax

clear multiauth trap {**system** | **module** | **port** *portstring* {**all** | **success** | **failed** | **terminated** | **max-reached**}}

Parameters

port *portstring*	Clears the configuration of multiauth port trap settings for the port specified in *portstring*.
all	Enables sending all traps for the specified port.
success	Enables sending success traps for the specified port.
failed	Enables sending failed traps for the specified port.

Downloaded from www.Manualslib.com manuals search engine

terminated	Enables sending terminated traps for the specified port.
max-reached	Enables sending max number users reached traps for the specified port.

Defaults

None.

Mode

Switch command, Read-Write.

Examples

This example shows how to disable the multiauth system trap setting:

```
Matrix(rw)->clear multiauth trap system
```

This example shows how to disable all multiauth port trap settings:

```
Matrix(rw)->clear multiauth trap port ge.1.1 all
```

show multiauth trap

Use this command to display multiple authentication trap settings for the specified context.

Syntax

show multiauth trap {**system** | **module** | **port** *portstring* {**all** | **success** | **failed** | **terminated** | **max-reached**}}

Parameters

port *portstring*	Displays the configuration settings for multiauth port traps for the port specified in *portstring*.

Defaults

None.

Mode

Switch command, Read-Only.

Example

This example shows how to display multiple authentication trap settings for port ge.1.1-4:

```
Matrix(rw)->show multiauth trap port ge.1.1-4
Location       Trap configuration
               Success     Failed      Terminated  Max-Reached
-------------  ----------  ----------  ----------  ----------
ge.1.1         Disabled    Disabled    Disabled    Disabled
ge.1.2         Disabled    Disabled    Disabled    Disabled
ge.1.3         Disabled    Disabled    Disabled    Disabled
ge.1.4         Disabled    Disabled    Disabled    Disabled
```


Downloaded from www.Manualslib.com manuals search engine

```
Matrix(rw)->
```

This example shows how to display multiple authentication trap system settings:

```
Matrix(rw)->show multiauth trap system
System : Disabled
Matrix(rw)->
```


Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

Index

Numerics

802.1D 6-1
802.1Q 7-1
802.1w 6-1
802.1x 25-54, 25-65

A

Access Groups 24-20
Access Lists 24-16 to 24-17
Addresses
  IP, adding to switch routing table 12-8
  MAC, adding entries to routing table 16-6
  MAC, setting for IP routing 16-17
  setting the router ID address 21-24
Advertised Ability 4-30
Alias
  node 14-1, 15-1
  physical 2-54
Area Border Routers (ABRs) 21-31
ARP
  entries, adding in routing mode 16-14
  entries, adding in switch mode 12-3
  proxy, enabling 16-16
  timeout 16-17
Authentication
  MAC 25-26
  MD5 21-30
  Multi 27-1
  OSPF
    area 21-32
    MD5 21-30
    simple password 21-29
  Port web 25-11
  RADIUS server 25-54, 25-57, 25-65
  SSH 24-12
  VRRP 21-70
Auto-negotiation 4-30

B

Baud Rate 4-5
Broadcast
  settings for IP routing 16-19
  suppression, enabling on ports 4-49

C

CIDR 21-13
Cisco Discovery Protocol
  configuring 3-8
Class of Service 8-8, 8-14, 8-21
Classification Policies 8-1
Classification Rules 8-7
Clearing NVRAM 2-97
CLI
  closing 2-92
  scrolling screens 2-10
  starting 2-7
Command History Buffer 11-1, 11-2
Command Line Interface. See also CLI
Configuration
  clearing switch parameters 2-97
  modes for router operation 2-103
Configuration Files
  copying 2-86
  deleting 2-87
  displaying 2-85
  executing 2-86
  saving or writing to output devices 16-9
  show running config 2-87
Console Port Settings 4-3
Contexts (SNMP) 5-3
Convergence End Points (CEP) phone detection 25-39
Copying Configuration or Image Files 2-86
Cost
  area default 21-34
  OSPF 21-24, 21-34
  Spanning Tree port 6-60

D

Debugging
  OSPF 21-50
Defaults
  CLI behavior, described 2-6
  factory installed 2-1
DHCP Server 20-1
Discovery Protocols
  about 3-1
  Cisco Discovery Protocol 3-8
  Enterasys Discovery Protocol 3-3
  LLDP and LLDP-MED 3-15
DoS prevention 24-22
DVMRP 21-52
Dynamic Egress 7-20

E

Enterasys Discovery Protocol
  configuring 3-3

F

Flow Control 4-37
Flow Setup Throttling (FST) 24-25, 25-60

G

Getting Help 1-2
GVRP
  enabling and disabling 7-26
  purpose of 7-22
  timer 7-27

H

H.323 detection 25-39
Hardware
  show system 2-35, 2-48
Hello Packets 21-28
Help
  context sensitive 2-9
  keyword lookups 2-9

I

ICMP 11-4, 16-27
IGMP 9-1
  enabling and disabling 9-2
Image File
  copying 2-86
  downloading 2-72
Ingress Filtering 7-9, 7-14
Interface Configuration Mode 16-3
Interface(s)
  configuring OSPF parameters 21-21
  configuring settings for IP 16-1
  RIP passive 21-15
  RIP receive 21-16
  RIP send 21-7
IP
  access lists 24-16 to 24-17
  address, setting for a routing interface 16-6
  addresses, adding to the switch routing table 12-8
  routes, adding in router mode 16-26
  routes, managing in switch mode 12-1
IRDP 21-55

J

Jumbo Frame Support 4-27

K

Keyword Lookups 2-9

L

License key
  advanced routing 2-58, 21-1
Line Editing Commands 2-11
Link Layer Discovery Protocol (LLDP)
  configuring 3-15
Link State Advertisements
  displaying 21-43
  retransmit interval 21-26
  transmit delay 21-27
LLDP
  configuring 3-15
LLDP-MED
  configuring 3-15
Lockout
  set system 2-23
Logging 10-1

Downloaded from www.Manualslib.com manuals search engine

Login
administratively configured 2-8
default 2-7
setting accounts 2-15
via Telnet 2-8
Loop Protect
about 6-2
configuring 6-65
Loopback Interfaces 16-1
LSNAT 18-1, 19-1

M

MAC Addresses
age time 12-11
displaying 12-10
setting in routing mode 16-17
MAC Authentication 25-26
MAC Locking 24-2
Management VLAN 7-2
MD5 Authentication 21-30
Mirroring Ports 4-51
MTU Discovery Protocol 2-90
Multicast Filtering 9-1, 9-2
Multiple Authentication 27-1
Multiple Spanning Tree Protocol (MSTP) 6-1

N

Name
setting for a VLAN 7-7
setting for the system 2-50
Neighbors
OSPF 21-47
RIP 21-4
NetFlow
configuring 15-1
versions supported 15-2
Network Management
addresses and routes 12-1
monitoring switch events and status 11-1
Network Statistics
displaying for switch 11-3
RMON 11-15
Networks
OSPF 21-23
RIP 21-3
Node Alias 14-1, 15-1
NSSA Areas 21-34
NVRAM
clearing 2-97
downloading configuration to 2-87

O

OSPF
Area Border Routers (ABRs) 21-31, 21-45
areas, authentication 21-32
areas, defining NSSAs 21-34
areas, defining range 21-31
areas, defining stub 21-33
configuration mode, enabling 21-22
configuration tasks 21-19
cost 21-24, 21-34
debugging 21-50
hello packet intervals 21-28
information, displaying 21-42 to 21-48
link state advertisements 21-43
neighbors 21-47
networks 21-23
priority 21-25
redistribute 21-37
retransmit interval 21-26
timers 21-26
transmit delay 21-27
virtual links 21-35, 21-48

P

Password
set new 2-18
setting the login 2-18
Path MTU Discovery Protocol 2-90
Phone detection
Cisco, Siemens and H.323 25-39
PIM 17-1
Ping 11-4, 16-28
PoE 4-13
Policy Management
assigning classification rules 8-7
classifying to a VLAN or Class of Service 8-8, 8-14
profiles 8-2, 8-21
Port Mirroring 4-52
Port Priority
configuring 22-2
Port String
syntax used in the CLI 4-2
Port(s)
assignment scheme 4-2
auto-negotiation and advertised ability 4-30
broadcast suppression 4-49
counters, reviewing statistics 4-15
duplex mode, setting 4-24
enabling and disabling 4-20
flow control 4-37
MAC lock 24-5
mirroring 4-51
priority, configuring 22-2
speed, setting 4-24
status, reviewing 4-13
Priority
OSPF 21-25
VRRP 21-64
Priority to Transmit Queue Mapping 22-5
Prompt
in router mode 2-103
set 2-44, 2-45
PWA 25-11

R

RAD 12-4
RADIUS 25-53, 25-63
RADIUS server 25-54, 25-57, 25-65
Rapid Spanning Tree Protocol (RSTP) 6-1
Rate Limiting 22-9
Redistribute 21-17, 21-37
Related Manuals xxxv
Reset 2-95
RIP
CIDR 21-13
configuration mode, enabling 21-2
configuration tasks 21-1
distribute list 21-17
neighbors 21-4
network, adding 21-3
offset 21-5
passive interface 21-15
redistribute 21-17
timers 21-6
RMON 11-15
Router Mode(s)
enabling 2-103
preparing for 2-100
Routing Interfaces
configuring 16-3
Routing Protocol Configuration
DVMRP 21-52
IRDP 21-55
OSPF 21-19
RIP 21-1
VRRP 21-61

S

Scrolling Screens 2-10
Secure Shell (SSH) 24-11
enabling 24-11
regenerating new keys 24-12
Security
methods, overview of 24-1, 25-1
Serial Port
downloading upgrades via 2-72
set policy classify 8-11
set policy port 8-6, 8-17
SNMP
access rights 5-18
accessing in router mode 5-3
enabling on the switch 5-20
MIB views 5-22
notification parameters 5-33
notify filters 5-33
security models and levels 5-2
statistics 5-5
target addresses 5-29
target parameters 5-26
trap configuration example 5-3
users, groups and communities 5-10
walk behavior 5-41
SNTP 13-1
Spanning Tree

Downloaded from www.Manualslib.com manuals search engine

bridge parameters 6-3
features 6-2
Loop Protect feature 6-2
port parameters 6-49
Rapid Spanning Tree Protocol (RSTP) 6-1
Split Horizon 21-15
Stub Areas 21-33
Syslog 10-1
System Information
displaying basic 2-34
setting basic 2-30

T

Technical Support 1-2
Telnet
disconnecting 11-7
enabling in switch mode 2-77
Terminal Settings 2-51
TFTP
downloading firmware upgrades via 2-72
Timeout
ARP 16-17
CLI, system 2-53
RADIUS 25-54, 25-65
Timers
OSPF 21-26
RIP 21-6
Traceroute
in router mode 16-28
Trap
SNMP configuration example 5-3

U

Updates
disable RIP triggered 21-14
RIP distribute list 21-17
User Accounts
default 2-7
setting 2-15

V

Version
RIP receive 21-7
RIP send 21-7
Version Information 2-48
Virtual Links 21-35, 21-48
VLANs
assigning ingress filtering 7-14
assigning port VLAN IDs 7-9
classifying to 8-8, 8-14
configuring for IP routing 7-2
creating static 7-6
egress lists 7-17
enabling GVRP 7-22
ingress filtering 7-9
naming 7-7
reviewing existing 7-3
secure management, creating 7-2
VRRP
authentication 21-70
configuration mode, enabling 21-61
creating a session 21-62
critical IP 21-66
enabling on an interface 21-69
priority 21-64
virtual router address 21-63

W

WebView 1-2, 2-7

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine